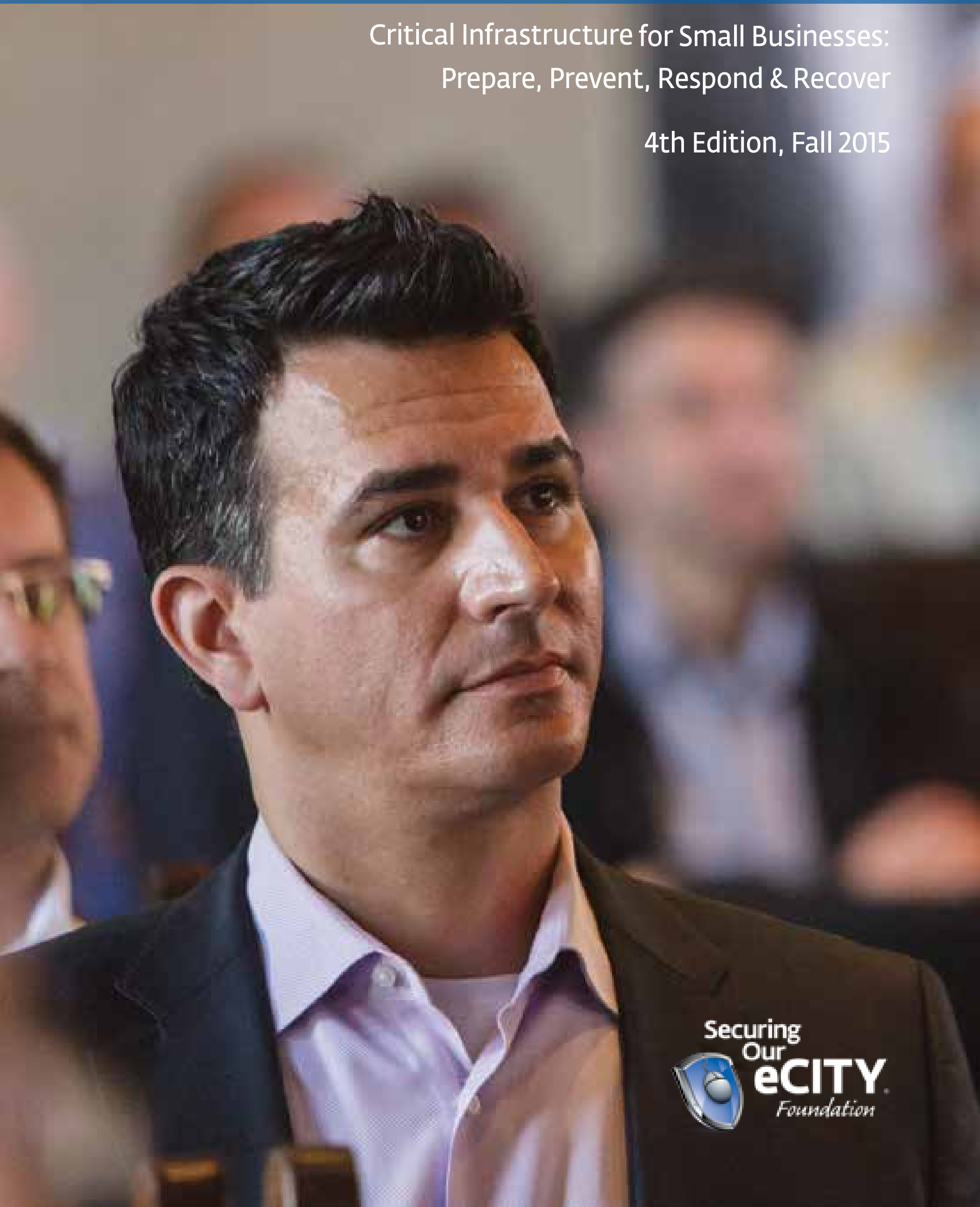
Bringing IT Home

Critical Infrastructure for Small Businesses: Prepare, Prevent, Respond & Recover

4th Edition, Fall 2015

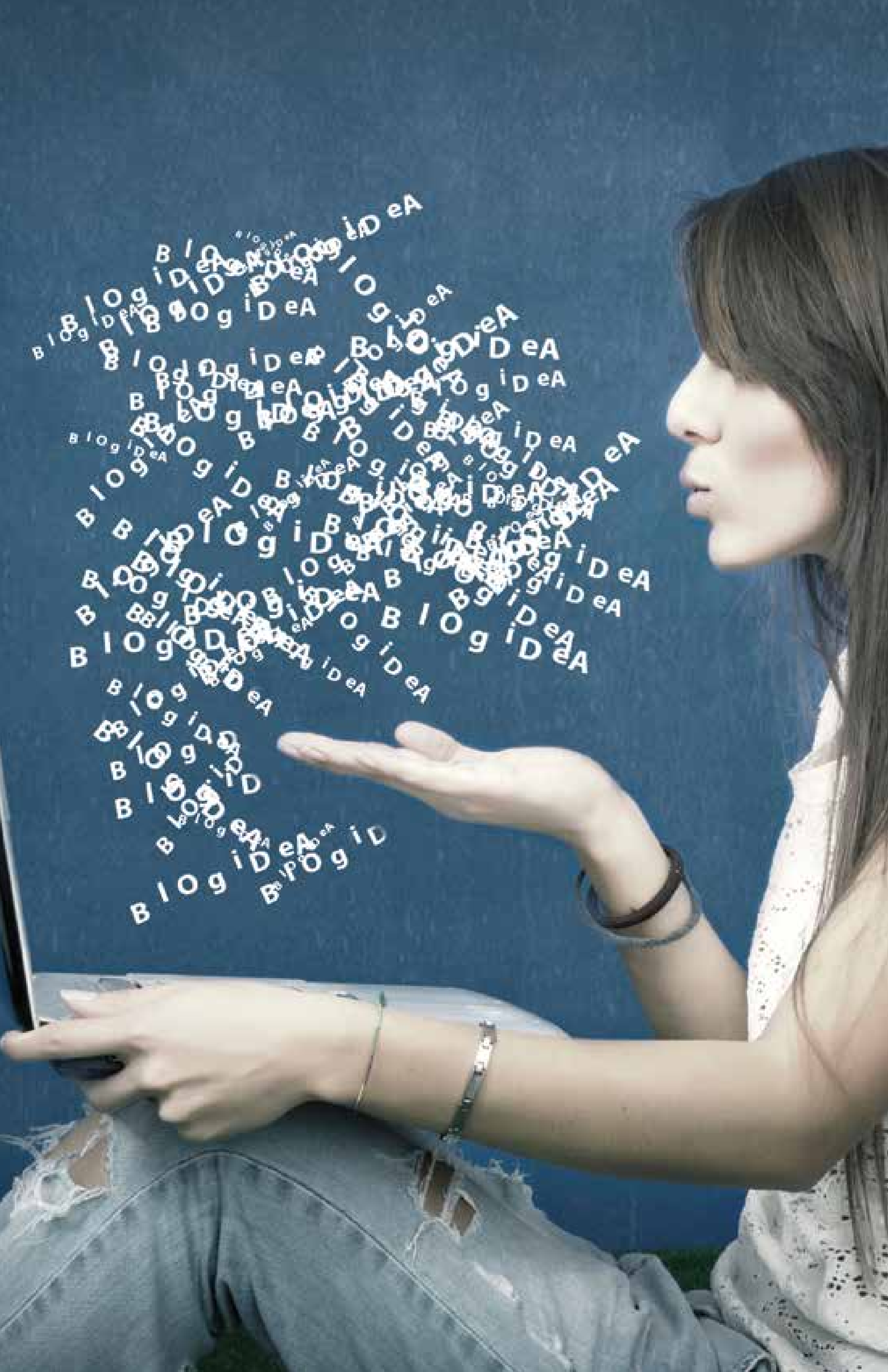


Securing Our eCITY Foundation

Acknowledgements

Thank you to the Securing Our eCity® Workgroups that have contributed their time and expertise to this effort.

Table of Contents


B l O g i D eA

Acknowledgements

Securing Our eCITY® Foundation wishes to thank the Critical Infrastructure (CI) Workgroup for their dedication and contributions to create this booklet, as well as other SOeC Workgroups who also contributed their time and expertise. Experts from many of the CI sectors and cyber security professionals worked diligently to help make a potentially very complex topic easy to understand for organizations of all sizes. It is extremely important that everyone, including SMBs, also understand they play a key role in the cyber security of our critical infrastructure, community, and nation. Thank you to all who have contributed and especially these key individuals:

Alan Watkins

Alexander Antrim

Alexis Madden

Brian Proctor

Cass Kelly

Chris Vera

Craig Hardin

Dan Green

Debi Preece

Derek Sandland

Ford Winslow

Gary Hayslip

Gary Martino

Liz Fraumann

Robert Burgett

Roger Fraumann

Rusty Sailors

With 50,000 security threats emerging each day, protecting your business is a serious job.

-XEROX.com , Feb. 2015

Introduction:
Critical Infrastructure and Your Business

As a business owner, you may wonder what is Critical Infrastructure (CI) and how it and Cybersecurity relates to your business. Especially if you are a Small or Medium Business (SMB), which make up 99.7% of all the businesses across the United States. Not only does CI affect our businesses, but it encompasses the very framework that is essential for all elements in our day-to-day life - both physical and cyber.

At a national level, there are sixteen industry sectors and at the San Diego regional level, InfraGard recognizes four additional subsectors that comprise CI. In this brief document, we will examine each of these key areas that are fundamental to our existence, and essential to our way of life across the United States. There are inter-related components, integral across nearly all CI sectors and those linkages may pose new threat vectors for businesses and individuals alike.

The keystone sector of our Critical Infrastructure is Energy. Without this key sector functioning, many, if not all other segments can be profoundly impacted. Municipal water flow may not be pumped through a community; transportation may revert to slow and obsolete methods; communication is virtually impossible; and modern food production and storage may cease.

In addition to the physical security, our energy providers focus on Cybersecurity in order to maintain the supply of energy. They also take extraordinary measures to ensure the integrity, safety, and security of their automated control systems and the “Smart Grid.”

Critical Infrastructure and Your Business

In this booklet, we provide scenario-based examples to help demonstrate the interplay between cyber and physical security measures that we suggest for consideration in a small-medium business environment. We propose these recommendations as a starting point for consideration, as you plan and prepare to keep your organization more cyber-safe.

If or when you believe one or more of your computer systems may have been compromised or breached, there are several pieces of information you should document in writing or gather from existing documents, to have on hand for reporting a cyber incident or for internal reference. In addition to using the detailed checklist of action items at the end of this booklet, you should try to capture the following information related to any potentially compromised/ breached systems:

- Current IP Address(es) of system(s)
- Use of dynamic (DHCP) or static IP address assignment
- Hostname(s) or NetBIOS Name(s)
- Operating System(s), including version and patch level
- Date and time of incident (discovery) and response
- Network Topology (how your systems are connected to each other and the Internet)
- Applications and processes running on compromised system(s)
- Estimated Impact (cost to restore/examine/investigate, lost customers and revenues, and brand impact)
- Applicable policies and procedures (what you have in place that are related to the compromise/breach)

What to Expect:

This booklet is divided into chapters for each CI industry sector, with a short description, followed by "Businesses in Action" giving real-life and realistic threat or attack scenarios, and then three subsections which cover sector-specific actions for "Prepare and Prevent," "Respond," and "Recover." Due to the common nature of responding to certain emergencies, there is noticeable overlap between CI sectors. The subsection headings are taken from standard Incident Management practices, and the intent of these subsections is explained below.

Prepare and Prevent

Planning, planning, and more planning – are you ever too prepared for an emergency? While a Cybersecurity incident may not rise to the level of other types of emergencies, such as natural disasters, it's not a matter of "if," it's simply a matter of "when" your business will become a victim of a cyber attack.

This Incident Management section deals with making risk-based business decisions, what steps should be taken to prepare for the inevitable, what security measures should be put into place to help make your business be less of a target, to prevent a successful cyber attack, and to minimize its impact to your business. This category includes implementation of necessary policies, procedures, and security standards, as well as training for employees and trusted partners who have access to your computer systems.

The following general action items apply to any business, with the expectation there will be differences in the level of detail and the manner of implementation.

- Create and distribute Cybersecurity policy and procedures document(s), including a Cybersecurity Incident Response Plan
- Educate all staff on safe Cybersecurity practices to help prevent an incident, and also on how to recognize and report a potential Cybersecurity incident
- Identify and avoid SPAM and phishing emails
- Use strong passwords or passphrases and biometrics properly, and consistently maintain them
- Recognize the latest social engineering tactics (e.g., "Spear Phishing" schemes)
- Only disclose personal or financial information on reputable sites and via a secure network

- Regularly confirm your company's compliance with internal security policies and any regulatory standards
- Be suspicious of any anomalous computer or network behavior
- Implement layered network and end-point security
- Identify where and what information resides on your network
- Backup your data from both local hard drives and shared network drives on a regular basis (e.g., weekly), and store an extra encrypted copy offsite
- Restrict access to resources and information to those who actually need it
- Image and/or retain hard drives from employees who leave under less than amicable circumstances or who had access to confidential data
- Enable computer and network logging, and store logs offline
- Treat every cyber incident as potentially malicious until it is determined otherwise

Respond

You have discovered a potential Cybersecurity incident, now what do you do? Do you already have Cybersecurity policies and procedures in place? Do you have a Cybersecurity Incident Response Plan – If not, then it's time to implement one! This Incident Management section covers the steps you should take when you have a potential or known breach, malware or other Cybersecurity incident. Even if it starts as unconfirmed, there are steps you can take which can prevent the spread of malware or reduce the impact of an intrusion, while in the process of confirming if an actual Cybersecurity incident is occurring or not. Once confirmed, there are additional steps to take to stop the attack, minimize or mitigate the damage to data or systems, and minimize the overall business impacts.

The following general action items apply to any business, with the expectation there will be differences in the level of detail and the manner of implementation.

- Contact authorities. Fast responses are important in cases with active data exfiltration such as customer or financial data
- Preserve the original hard drives of compromised systems
- Provide documentation for anything that has been done to the system since the discovery of the incident
- Provide copies of any network diagrams or system documentation showing the environment in which the system operated
- Identify and copy any internal or external log files (i.e. intrusion detection system or firewall logs)

- Consider monitoring the system's network connections prior to taking it offline. Other compromised systems or suspect IP addresses can frequently be identified

Recover

The incident is over and your business may have suffered minor, moderate or major impacts. How well did you Prepare and Prevent, and then Respond to the incident?

> 70% of all small businesses that experience a major data loss are out of business within one year.
>
> - SBA, 2010

Even with proper preparation and response, steps must still be taken to get the business back to normal operations. This final Incident Management section provides certain steps to take, to help keep the business running during the immediate aftermath of an incident and then continuing to fuller recovery. It should be noted that, even with the best planning, preparation, and response, a major Cybersecurity incident could cause catastrophic, unrecoverable damage to a small/medium business. Following the basic steps outlined above and in this booklet are intended to increase a business' chances of being able to recover and restore operations. Depending on the nature and scope of the incident and the type of business you have, temporary operations may be restored within several hours or sometimes days; maybe working out of a vehicle as a mobile office. A more stable, partial recovery and restoration of business operations may take several days or weeks; while a full recovery may take weeks or even months.

The following general action items apply to any business, with the expectation there will be differences in the level of detail and the manner of implementation.

- Find a safe place to re-start operations – this might be the normal office space, if there was no disaster which caused physical damage; or this might be an alternate location, set up temporarily to be able to conduct business

- If you are unable to use your computers (e.g., network services are not available), and the nature of your business allows it – conduct business manually and keep track of all transactions on paper

- If computer equipment was damaged or is being kept as evidence, arrange to lease or buy new computer equipment, and have it installed and configured for your business use. Consider getting Cybersecurity insurance (before an incident occurs), to help pay for replacement equipment and data restoration

- If you will be using existing computers, ensure they have been "cleaned" of any malware; reformat the hard drive and reload a clean image of the operating system, then install software applications

- Restore your backup data to the point before the computers were infected or breached; test and validate the data before resuming operations with it; be sure to add any manual transactions into your system to get it up to date
- After restoring your computers and business data, make a fresh backup of each system; store one copy at the business and store a second copy off-site in a secure place (i.e., in a locked fireproof cabinet)
- Notify your vendors, suppliers, distributors, customers, and other stakeholders when you resume online operations, even if it’s from a temporary location

Our food supply chain is closely tied to our power grid. For example a loss of power can lead to ultimate starvation.

-Communications of the AMC

Energy

For the purposes of this document, we consider energy as the foundation for all critical infrastructure. An interruption or loss of power has the potential to impact all other sectors of CI. While alternative sources of power are available and in some areas where they have been implemented on a case-by-case basis, it is the overarching power-grid on which we base our daily lifestyle and business practices. More often than not, without power there is no communications, fuel, transportation, healthcare practices and on and on goes the list.

As with all sectors of our Critical Infrastructure, energy planning, policies and procedures will help businesses and individuals more easily survive, if an emergency situation arises.

We are fortunate to have an organization like San Diego Gas & Electric supply our power and offer tips for both businesses and families alike on how to prepare for a "blackout." For more information, you can visit:

http://www.sdge.com/safety/emergency-preparedness/preparing-emergency-one-happens

Examples for Energy:

- Power Consumption Monitoring
- Peak Power – Backup Power Generation Management
- Emergency Power Generation Systems
- Fuel Supply Management for Emergency Generators

Family Health Center of South Bay

On a warm, sunny afternoon in early September in San Diego, the South Bay Family Health Center was humming along as usual. The examination rooms were full with the usual patient load. The waiting room seemed to be full as well, but it was the beginning of flu season and a flyer had been distributed promoting the shot clinic. So, it was a "good thing." At 3:40 PM it all seemed to just fall apart – the power in the entire facility was gone. No lights. No air conditioning. No computers. No oxygen. No locks – nothing was working. Nada!

The emergency team gathered to assess the situation and size-up the scope of the issues, while the nursing staff retrieved flashlights and attempted to keep the already stressed patients calm. It wasn't working too well. As time went on, new people, frail and ill showed up at the Health Center looking for help. The challenge? Little could be done, as there were no means to see in the interior of the building as the day wore on to evening and nightfall.

Without access to the computers and the database, transfers were next to impossible. We learned later that the whole county experienced the same thing.

It was time to implement the plan we trained and practiced for and pull out our generator to see what we could do to help our patients and others that appeared to be a stream of humanity looking for help.

Sporting Goods Store

Bob and Sue Williamson own and operate a sporting goods retail shop in San Diego. The majority of their sales are processed with credit or debit cards and they keep their inventory, employee information, and supplier contact details on their computers.

After a friend's suggestion, the couple invested in an uninterruptable power supply and backup system. A few weeks passed and they wondered whether the purchases were a waste, when suddenly the power went out in the store. A local transformer had fallen victim to a car crash, failed and power dropped in a 10-mile radius. Sue panicked because an important customer was just about to make an enormous purchase. Luckily, the cash register was still running, so she had the customer write a check and she processed the order, making a huge profit that might otherwise have been lost. With sixty minutes of power to wind down, Sue and Bob finished taking inventory and safely shut down their computers while other local stores lost large amounts of important information. All of their data was available on the backup drives and when power returned the next day, they continued business without a hitch.

Prepare and Prevent

The best way to limit a potential business impact due to power loss or data breach is preparation. The first steps in preparation begin with planning and policies. If you have a plan and policies, review them on a regular basis to ensure all information is current and in-line with current best practices. If your staff is not up-to-date on your policies and procedures, or forget to regularly check systems and prepare for an unexpected disruption in services, the impact can be great. If you have emergency generators, test them at least quarterly.

Consider part of the planning process to look at your business life cycle and key dependencies. You should also build alternative sources and relationships so they are at the ready, should it become prudent or necessary.

Respond

In the event of a power outage, ensure your staff and guests' safety first. Consider alternative communication devices and develop a plan where staff who may be off-site can be informed about working conditions and updates as to whether they should come in to work. Consider incorporating a Uninterruptable Power Supply (UPS) to allow appropriate, safe, coverage for critical information systems at your work or home. Unplug sensitive machines, so when power returns they are not affected by a power surge.

If you encounter a cyber-incident, you need to contact the authorities. Call your local police or FBI and submit the issue to the Internet Crime Complaint Center (IC3) at http://www.ic3.gov/complaint/. Document your observations before, during and after incidents. Preserve the hard drive and, take any affected system offline to minimize the possible spread and damage to other systems. Document all information about your network information and policies. See *Into the Breach* from the Securing Our eCITY® Law Enforcement workgroup.

Recover

If the power is down for an extended period of time, you will need to weigh your options carefully. Statistics from the SBA in 2010 show that 70% of small businesses that experience a major data loss do not survive the next year. However, you can mitigate this risk with proper planning, policies and preparation. During your initial recovery period, do your best to use cash transactions and document everything on ledgers. Once the power returns, recover your vital information from backup servers and notify customers appropriately. In California, Civil Code §1798.29 & §1798.82 dictate specific procedures if data has been breached or leaked. We recommend that SMBs become familiar with all local, state and federal laws as it relates to data and data privacy. Check the Securing Our eCITY® web site for workshops and resources that can help you better understand the laws. Be sure to destroy and dispose of old data responsibly and effectively.

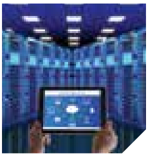
Chemical (Research & Biotech)

The Chemical industry produces a broad spectrum of products including basic chemicals, specialty chemicals, agricultural chemicals, pharmaceuticals, and consumer products. This sector relies on and also supports several other critical infrastructure sectors.

It is an industry which classically may make large investment in physical plants that are expected deliver 24/7 over multiple decades. As a result, embedded process control systems can remain in place with little or no changes. Meanwhile, business models advance at a faster pace, often impacting end user customer service and order management, which outstrips and cocoons the embedded process control technology. Demands for advanced machine-to-machine communication protocols, smart manufacturing, and predictive maintenance, also apply significant pressure on the already strained IT infrastructure.

Examples for Chemical:

- Materials Management Systems
- Product Composition Analysis – Lab Testing Systems
- Automated Production-Line Systems (i.e., Packaging)
- Vendor/Supply Management Systems
- Quality Control / Quality Assurance Tracking Systems



Just-In-Time Chemical Material Delivery

MegaChem has several constant-flow chemical production systems operating 24/7, and any unplanned interruption of key material delivery may result in abnormal shutdowns and resultant spill potential. MegaChem replaced their point-to-point EDI (Electronic Data Interchange) system with a data brokering service provided by ChemCloud.

MegaChem contemplated saving considerable costs by not having to support multiple dedicated EDI resources and skills. However, this change introduced a new supply chain vulnerability, where providing just-in-time information regarding key material delivery data now has a more tortuous path through additional networks, firewalls, the Internet, and ChemCloud's infrastructure-in-the-middle. When ChemCloud's managed data center became the target of a significant, Distributed Denial of Service (DDoS) attack, data was delayed and corrupted, resulting in mandatory shutdown of key production processes within MegaChem.

As a result, MegaChem had to reconsider its use of cloud services and look for alternatives to ChemCloud which might provide more secure and stable systems that meet their requirements for the chemical industry. One new requirement was the addition of a legal liability clause related to provision of hosted data services. MegaChem also had to update its process control procedures to include contingencies for a similar type of event.

Chemical Process with Linked Analysis Hardware

SpecChem is a specialty chemical company utilizing an Advanced Process Controller to manage a portion of their chemical production system. The controller, in turn, relies on data from a process mass spectrometer which analyzes the production stream. This investment enables them to remain nimble while addressing changing production and supply requirements; providing a significant competitive advantage.

Their Advanced Process Controller is maintained as a hardened and fault-tolerant system and, when they replaced a failing process mass spectrometer, the new unit called for a software driver update. The manufacturer provided a link on their website for the customer to download the latest driver.

Unknown to the spectrometer manufacturer, their website had been hacked, and a modified software driver was substituted, which in turn was subsequently downloaded by unsuspecting spectrometer customers. While the manufacturer provided an MD5 signature value adjacent to the driver web download button, the SpecChem system administrator failed to take the step to compare and validate the MD5 hash value of the new driver with the MD5 supplied by the manufacturer.

The hacker had modified the driver to cause, in certain situations, abnormal fluctuations in certain values within the protocols passed to the process controller. As a result, external safety mechanisms triggered, but not before damaging key plant production equipment, which in turn caused SpecChem to miss delivery deadlines and subsequently lose key customer accounts, and suffer significant negative brand impact.

The SpecChem system administrator who failed to check the MD5 hash was fired for negligence and, despite the employee's improper actions, SpecChem is planning to seek remuneration for some of the damages from the spectrometer manufacturer. A new procedure was implemented for software updates on all systems, especially those related to process controls, which requires a double-check by a second system administrator before it's installed, to ensure the software is the proper one for the particular system and is free of malware.

Prepare and Prevent

Planning for safety and prevention of environmental hazards is part of running a business which uses potentially dangerous chemicals, and the pervasive use of technology in operations requires that Cybersecurity be part of any such plans. In these example cases, the small business was not a direct target of a cyber attack, yet fully felt the consequences when their service providers were victims of different types of attacks. Supply chain interactions, production line automation, and distribution channels must all be included, now more than ever, because of the digital inter-dependencies between companies and even customers. This means the business needs to coordinate emergency operations and incident response plans with its suppliers, vendors, partners, distributors, and others (such as IT service providers).

Failsafe and manual procedures must be incorporated into an Incident Response Plan, which may include shutting down certain functions or operations. To help prevent unauthorized take-over of automated equipment, it should not be on the same network as office systems and consider not allowing Internet access to or from the devices. This would require any software changes or updates to be done with a secure laptop (one that has layered security controls installed) which must be physically connected to a device and requires valid user authentication for access. The secure laptop should not have any wireless or wired connection to any other network or the Internet while it's being used to update the automated equipment.

Respond

Hopefully, there is an emergency response plan (or incident response plan) which will be activated when a potential cyber attack or other threat has been identified. Follow the necessary steps to identify the target system(s), then stop the attack if possible (e.g., quarantine the impacted systems off the network), prevent the spread of malware or active intrusion/breach to other systems in order to minimize impacts to business operations, and take action to shut down any operational processes affected by the incident. Follow any regulatory compliance procedures to notify appropriate agencies, and make sure employees are following emergency safety protocols. Keep in mind the potential need to preserve evidence of the incident, which might mean removing and storing the hard drive(s) in a secure location, as well as saving all relevant log files (system logs, network logs, security monitoring logs, etc.). If production systems have to be shut down, notify suppliers to suspend delivery of products or materials until operations resume.

When the incident is under control, not necessarily resolved, take a quick inventory of assets – which ones were impacted and those that were not – including hardware (servers, desktops, laptops, network devices, etc.), software, process control systems, and ancillary systems (e.g., door access, security, CCTV). Document any anomalous activity or performance on systems or equipment that may be related to the incident. Share relevant information, as required, with law enforcement or regulatory agencies.

Recover

It's usually not feasible for SMBs in this CI sector to have a stand-by location for temporary operations in the event of an emergency. This means the business needs to plan for taking steps to facilitate recovery of operations at its normal location. It's also usually not feasible to have duplicate equipment stored onsite or nearby for swap-out replacement when production equipment fails. However, it should be feasible and financially possible to have a reasonable supply of critical spare parts, which may include computers or components (e.g., spare hard drives). Part of preparing for recovery in this case, is having an accurate and complete inventory of equipment and other assets, including lists of internal components/parts and which ones are considered critical enough to obtain spares.

Once an incident is over, the business needs to conduct a quick assessment of what will be needed to restart operations. This includes, but is not limited to, hazardous materials clean-up, raw materials and supplies, equipment repairs or replacement, personnel, computer systems (either for automation controls or for administrative uses), and necessary services (such as network and communications). Address and resolve all safety issues first, then there should be a logical plan of action for the steps needed to resume operations. Use the contracts and procedures previously developed with suppliers, vendors, partners, and other service providers as a joint effort to facilitate recovery.

In many cases, the chemical industry threats are unseen and yet pervasive. A change in the "mix" can result in toxic threats. Without secured, computer controlled devices, the potential for catastrophic events is greatly increased. Trusted sources and controls are essential in this industry.

Investment ma

Commercial Facilities (Tourism & Public Venues)

An often-overlooked sector of our Critical Infrastructure is Tourism, including Public Venues. This area can be targeted in order to weaken a city's economy or damage the reputation as a prime destination spot. Hotel chains and travel agencies can be hacked, losing valuable personally identifying information; airports can be targeted, effectively stalling travel; amusement parks can be penetrated, creating real and physical danger for unsuspecting visitors.

Areas where people gather within a city, whether tourists or residents, must take extra precautions to protect their "guests" in order to continue to provide a safe and reliable form of entertainment and relaxation.

Most cities rely on some form of tourism as an important source of revenue. From the smallest town, with bed and breakfasts, to the large metropolis, with golf resorts and global convention centers, they all rely on tourism. All forms of tourism are vital to bringing in visitors, to enhance the diversity of the community and increase the economy. If this area is subjected to a cyber-attack, the overall reputation of the associated organizations and even the entire community can be negatively affected and experience an economic downturn.

Examples for Commercial Facilities:

- Event Management Systems
- Traffic Planning & Management Systems
- Facility Management Systems
- Customer Services & Support Systems
- Access Control & Security Systems

Travel Abroad, Inc.

John Alcott owns a small travel agency catering to visitors to the city. He works with counterparts in other cities around the country to plan travel packages to visit his city. The database he maintains is connected to a large travel system that pulls traveler data from other agencies, so that he can better cater to their travel needs.

One morning upon arriving to his office, he immediately started working on a travel package for an elderly couple from Iowa. They wanted to stay in a four-star hotel on the beach and obtain fine dining reservations for every night during the trip. John tried to log into the shared client database and found that he was locked out. He contacted the system administrator for support and learned the support office was in a panic. Someone had used his workstation to access the database and locked everyone out of the systems.

Gigabytes of data were stolen out of the system. This included clients' personal identifiable information such as passport numbers, driver's license information, credit card information, and more. John did not understand how his workstation could have been the doorway to this crime. What could he have done to prevent this?

BuildingBlock Castles

BuildingBlock Castles is one of the most popular amusement parks in the area. This park is home to various miniature sculptures of famous sites around the world. It also has three rollercoasters and seven water rides. As more and more of these rides rely on technology, they can become potential targets of cyber-attack as well. Their control systems require security to protect the safety of BuildingBlock Castles visitors; a number one priority for their staff.

The park also has a large database containing season ticket holder financial and personal information. And, it maintains a beautifully designed website linked to the other BuildingBlock Castles parks around the globe. If any of these areas were to be breached, the outcome would be disastrous. Even a small data loss could cause the shutdown of the park and possible closure due to the financial impacts.

Visitors need to know that their information is safe and protected. No one will want to visit an unsafe park digitally. What can the park do to protect its visitors?

Prepare and Prevent

Data loss recovery plans are one of the first steps to rebounding from any incident. Establishing an offsite backup service can help ensure data can be restored in the event of a failure. Additionally, antivirus programs should be mandatory on all devices, and additional monitoring by experts can help, particularly with larger networks.

Lastly, safety locks should also be used on any equipment that might be dangerous to people. In the case of a control system takeover, the equipment should immediately shut down so that people can be evacuated safely.

Respond

Whether the people involved in an incident are visitors or residents, safety is the number one focus for any community. Depending on the size and scope of the incident, leading practices should be implemented including executing your incident communications plan to customers, supply chain and vendors; disconnecting systems as appropriate from the Internet to stop potential spread of a breach; and reporting the incident to appropriate authorities (potentially including the FBI). Sharing with the local government officials may be appropriate, again depending on the size and scope of the incident. It is much easier to rebuild a community's reputation together than pointing fingers at each other.

Recover

A recovery from an incident can be accomplished if the correct planning is done. All affected parties that have been impacted need to be contacted directly to maintain any future relationships. Only the nurturing of these relationships can rebuild a positive reputation as a travel destination.

Communications

The Communications Sector[1] is an integral component of the U.S. economy, underlying the operations of all businesses, public safety organizations, and government. Presidential Policy Directive 21 identifies the Communications Sector as critical[2], because it provides an "enabling function" across all critical infrastructure sectors. Over the last 25 years, the sector has evolved from predominantly a provider of voice services into a diverse, competitive, and interconnected industry using terrestrial, satellite, and wireless transmission systems. The private sector is the primary entity responsible for protecting sector infrastructure and assets. Working with the federal government, the private sector is able to predict, anticipate, and respond to sector outages and understand how they might affect the ability of the national leadership to communicate during times of crisis, impact the operations of other sectors, and affect response and recovery efforts.

In 2013, the Telecommunications & IT (T&IT) sectors in San Diego were responsible for nearly 2,000 businesses and more than 65,000 jobs[3] in the County of San Diego. The combined T&IT industry segments generated approximately 179,020 jobs and $38.11 billion annually in direct and indirect economic activity in 2010. This output was equal to 22% of San Diego's GRP for 2010, and every $1.00 directly invested in the telecom industry here in San Diego resulted in an additional $1.70 of economic activity in the region.

[1] http://www.dhs.gov/communications-sector

[2] http://www.ise.gov/mission-partners/critical-infrastructure-and-key-resources

[3] http://workforce.org/sites/default/files/pdfs/reports/industry/01_08_13_telecom_report.pdf

SD Medical

Karen works in the customer support call center for a large medical billing company. She handles customers who call in with problems concerning medical billing and the way in which the bill was charged to their credit cards – it is a very busy call center and she leads five of the 38 people on her floor of the building. Karen is on a call with a man who is rather upset because he hasn't gotten his problem resolved after his previous three calls with the center – this is now his fourth call. Karen is explaining her approach to address his problem when he stops responding in the conversation. Karen notices that her phone has gone dead! As she turns to Mike in the next cubicle to complain about her phone, she sees that Mike has lost contact with his customer as well. Suddenly the extension lights begin flashing on Karen's phone, and moments later, random phones begin ringing throughout their call center. What is going on? One of the lead administrators in IT had been laid off the week before for running his own business on the side during business hours and while he was at work. He thought it would be funny to get back at the company by hacking the VoIP phone systems – he wasn't an engineer, but with a little bit of research and just a few lines of code he was able to put in a simple back door that gave him full access to listen in or play with the phones as much as he wanted to.

Smith Financial

Michael runs a financial planning firm, and it's tax season so everyone is contacting his account managers about last minute changes they can make to reduce their taxes. The phones won't stop ringing and emails are piling up. It's great for business to be this busy, but the load is getting pretty heavy for his staff of five professionals – at least they're still staying ahead of the game. As he's walking back to his office to help the next client, he hears Megan saying something about the phone being cut off. Ryan stands up and exclaims, "Hey, my Internet is gone!" All five account managers confirmed their phones are off and they have no Internet access.

Michael finds out that a backhoe at a nearby construction project has cut through a major fiber-optic network that feeds the section of town where Michael runs his firm. With everything going on and the customers needing immediate support, things are looking bad for Michael's small business! Allie says, "Hang on – we know how to handle this! We covered this in our plan." Allie goes to the supply closet and pulls out six boxes that contain hot spot kits for everyone's company smartphones and computers. She calls on her phone and activates the six accounts that have been standing by. Within a few minutes everyone has Internet service via their respective "hot spots" and begin informing their clients to use email or their cell phone numbers to reach them until the emergency is resolved. Planning ahead of time worked for Michael and his small financial planning business.

Prepare and Prevent

Develop a Disaster Preparedness and Response Plan that cover both physical and virtual critical incidents and emergency situations. Within the context of that plan, develop an easily understood response process for communications that people can readily follow while stress is high and nerves are fragile. A solid simple plan with easy-to-follow processes can provide a level of stability and assurance when many people are in a stressful situation.

Educate and train your people. Emergency training drills may not sound much fun and may seem as though they can take time away from generating revenue, but if done properly, training and education can build confidence and be fun and rewarding. Find champions on your teams and give them responsibilities to be a part of the training and education. Be creative in the ways in which you share information that could otherwise be dry and uninteresting. Handing out a flyer or a training manual and requiring a signature that your staff has read it won't really help very many people.

Respond

If an emergency event occurs and your standard forms of communications are unavailable, there are several important things you can do in response.

- First and foremost is safety – make sure everyone is accounted for and you have a move forward plan that keeps everyone as safe as possible.
- Remind your teams of the emergency response plans and processes – ensure you have hard copies they can access if electronic systems are down or the Internet is unavailable.
- Give your staff assurance that your company has prepared for such an event and you have alternative capabilities and processes in place they can use.
- If your communications event has been caused by a cyber-related event, closely follow your emergency response procedures. There are many potential legal issues involved and challenges to address concerning electronic Discovery (eDiscovery) of ESI (Electronically Stored Information) and its potential use as evidence in court. You should also follow your emergency procedures to minimize the impacts of spreading the effects of the cyber event. Your procedures should be developed with your systems in mind so your recovery is safe and timely.

Recover

Ensure you have a plan for business resilience that addresses loss of critical infrastructure including the wide range of communications. When communications are down, many other areas can be affected, including:

- It is highly probable that the duration of the emergency event will strongly affect your ability to recover and the rate at which you will recover. However, even short events can have long-term effects if they are severe. Prepare for extended outages and your ability to recover will be much more effective. Evaluate what it takes to keep functioning for 1 hour, 4 hours, 8 hours, 24 hours, 48 hours and even longer. Consider developing a response plan for these durations that is risk driven and considers your budget.
- Prepare an emergency fund from which you can draw on during challenging times. Make sure you can gain access to it if communications with financial institutions are affected.
- Physical damage to systems can be very expensive and difficult to recover from. Be sure to work with your legal, financial and insurance professionals to understand your options and avoid making mistakes that could be costly and difficult to recover from.
- Cyber events can be very difficult and expensive, because they can be very damaging and it can be hard to fully identify the source and extent of the event. If you have a complex event with potentially long range and expensive recovery impacts, contact the FBI and ask for their help. In doing so, be very specific about the incident and share information and access to systems directly involved in the incident. They are experts at what they do and may help you get back on track earlier and resolve potentially longer-term issues faster.

At the heart of any relationship, business or personal, is communications. In today's world of split second decision making and information exchange, businesses require trusted and reliable communications for continued success and, in some cases, life of the organization.

Critical Manufacturing

The Critical Manufacturing Sector focuses on the identification, assessment, prioritization, and protection of nationally significant manufacturing industries within the sector that may be susceptible to manmade and natural disasters. The sector is crucial to the economic prosperity and continuity of the United States. A direct attack on or disruption of certain elements of the manufacturing industry could disrupt essential functions at the national level and across multiple critical infrastructure sectors.

The following industries to serve as the core of the sector. Products made by these manufacturing industries are essential to many other critical infrastructure sectors.

- **Primary Metal Manufacturing**
    - Iron and Steel Mills and Ferro Alloy Manufacturing
    - Alumina and Aluminum Production and Processing
    - Nonferrous Metal (except Aluminum) Production and Processing
- **Machinery Manufacturing**
    - Engine, Turbine, and Power Transmission Equipment Manufacturing
- **Electrical Equipment, Appliance, and Component Manufacturing**
    - Electrical Equipment Manufacturing
- **Transportation Equipment Manufacturing**
    - Vehicle Manufacturing
    - Aviation and Aerospace Product and Parts Manufacturing
    - Railroad Rolling Stock Manufacturing

National Cyber Solutions

On Monday morning, Larson Klein arrives at his workplace, brews some coffee, and makes his way to his office space to turn on his computer. Lydia, Larson's colleague, heads to the restroom before turnover with Larson. Larson and Lydia work for National Cyber Solutions, a company that provides a contractor owned/contractor operated (COCO) network and services for the DoD logistics command. Larson's and Lydia's primary responsibility within the company is to monitor a dashboard that displays alerts for processing, shipping, and delivering military goods. After turning on his computer, Larson sits at his desk and logs onto the system.

The system is not the quickest to authenticate to and gain access, so Larson waits patiently as the dashboard eventually loads; however, unlike yesterday when the dashboard was colored with yellow, green, and red lights, signaling the movement and transportation of goods - today none of the lights appear and no information is displayed. So, Larson calls for Lydia. Lydia had recently been passed over for promotion and subsequently made several open comments about how she is not happy with the company. When Lydia returns from the restroom, she promptly grabs her purse and tells Larson she has to hurry home. As Lydia slams the door and exits the office, Larson looks down at the computer - discovering a USB thumb drive inserted in the computer. It is company policy that all USB devices are unauthorized for use. Immediately following the discovery, Larson calls his supervisor and informs her about the system dashboard, reports the observed behavior by Lydia and her lack of turnover, and the USB thumb drive inserted into her workstation.

The supervisor promptly initiates failover capabilities, and an alternate site work team takes over network monitoring. After further investigation by the National Cyber Solutions' Incident Response Team (IRT), it was discovered that the inability for the dashboard display to operate was due to a Denial of Service (DoS) condition created from malware infiltrating the network. The IRT investigation revealed that the malware traced back to Lydia's USB thumb drive. The malware exploited multiple software vulnerabilities within the network and established a presence within the network. Once the malware was up and running, it received automated updates, allowing someone on the Internet to access the National Cyber Solutions network. This loss of control for the National Cyber Solutions network was a direct result of commands executed by programs Lydia had installed via the USB thumb drive, which automatically self-replicated multiple copies of the malware, further infecting the network. Lydia's actions reflected the realization of management's worst fears about trusted employees becoming insider threats.

The aftermath of Lydia's actions led management to re-assess its security posture and implement additional control measures. USB thumb drive ports were disabled and made inaccessible on all devices, the "autorun" feature was disabled, and user account settings were reconfigured to least privilege access. The implementation of administrative, technical, and physical security controls created an improved, layered security approach. Implementing security controls through a layered approach makes it more difficult for a malicious entity to disrupt the confidentiality, integrity, and availability of the company's information. The implementation of additional security controls, both physical and logical/digital, can help to better prevent, detect, and respond to security incidents. Improved incident prevention, detection, and response equates to less company liability and expense, increased productivity, and the ability to continue operations in the event a security incident does occur.

Prepare and Prevent

As with any production-oriented business, preparation must include operational and emergency plans, usually including manual processes in case of automated systems failure. As far as the manual operations procedures to follow in the case of a failure, it shouldn't matter what the cause was, however, actions taken to respond to a possible cyber attack involve several necessary steps that would not be taken in the case of an accidentally misconfigured system.

Plans and procedures need to address the supply chain, production, and distribution aspects of the business. There should be pre-determined processes agreed to between the business, its suppliers, vendors, service providers, and distribution channel partners in the event of automation failures and switching into a manual mode. If certain production processes must be shut down, that needs to be taken into account in the plans and procedures. If there are any regulatory compliance issues related to operating in manual mode, the business must coordinate its plans and procedures with the regulatory agency.

If possible and practical, maintain redundant, backup systems (which can be offline until needed) for critical production systems. Make regular backups of system configurations, in case the backup system needs to be brought into operation. Also make regular backups of data files, which may include customer information, company administrative information, accounting and billing information, etc.; and store a copy of the backup offsite in a secure location. Make sure systems are automatically updated with security patches and use a combination of firewalls, anti-malware, and other security measures to protect both servers and end-user systems. Keep all production systems on a separate network from the office administrative systems, and do not permit Internet access to production systems.

Respond

Once a cyber security incident has been identified, implement the procedures in the Incident Response Plan, which should include isolating any impacted systems, securing physical process equipment to ensure everyone's safety, activating procedures to mobilize an Incident Response Team (IRT), starting necessary notifications regarding the incident (e.g., suppliers, vendors, partners, law enforcement, company management, etc.), taking actions to find the cause of the incident, and potentially taking impacted systems offline to prevent further spread.

If necessary, remove impacted systems and follow procedures for preserving evidence, in case they are needed for future legal action or insurance claims. Prepare to restore operations of critical equipment by installing and activating any backup or standby systems available. Once the incident has been brought under control, start validation checking of all critical systems, both operational and administrative, to ensure there is no hidden malware and no other file corruption or damage was done. Prepare to restore backup data to impacted systems, or to new systems that might be purchased to replace ones that are being held for evidence or cannot be cleaned of malware.

Recover

When restarting business operations, first ensure that all safety issues have been addressed and resolved. Notify appropriate staff regarding work locations and job assignments, which may involve an alternate work site and include setup and configuration of standby or new systems. As operations are brought back online and functioning properly, notify suppliers, vendors, distributors, and customers, to advise them of any temporary changes in normal operations and business processes, and ensure everyone understands the expectations for how the business will function until operations are fully restored.

Coordinate and cooperate with any necessary follow-up activities with law enforcement or regulatory agencies related to the incident. After restoring backup data to impacted or replacement systems, create another new backup of the data and system configurations, then store one copy onsite in a secure place and a second copy offsite in a secure location.

Trusted business partners are key to any organization's success. It is knowing, understanding, and assessing how they must rely on each other for day-to-day operations, communications and the manufacturing of goods, that builds strength and trust in the partnership.

Dams

With over 87,000 dams in the United States, nearly two-thirds (65%) are privately owned and operated. This sector includes hydropower generation facilities, navigation locks, levees, dikes, hurricane barriers, mine tailings, other industrial waste impoundments, and other similar water retention and water control facilities. This vital part of the nation's infrastructure provides economic, environmental, and social benefits, including hydroelectric power, river navigation, water supply, wildlife habitats, water and waste management, flood control, and recreation.

The use of technology has broad applications across the wide spectrum of services and activities related to dams, ranging from water quality control and flood warning systems, to power generation monitoring and wildlife observation.

Examples for Dams:

- Industrial Control Systems (including Supervisory Control and Data Acquisition (SCADA) systems) for managing hydroelectric equipment or water treatment processes
- Water level monitoring and control systems, to manage release of excess water through spillways, and which may include flood warning systems
- Security video surveillance systems
- Water quality analysis systems
- Permitting systems for managing access into certain recreation areas

Local Environmental Testing Company

Sarah, a biologist with Southwest Environmental Analysis, Inc. (SEAI), is responsible for collecting water and plant samples from two dozen sites around a local dam and reservoir, to track water quality and any changes in plant health and growth. The dam is operated by the regional water authority, which contracts several services to small/medium businesses, including regular, ongoing environmental monitoring by SEAI. The reservoir is closed for all water contact types of recreation; however, fishing from the shoreline is allowed.

During a normal week, Sarah collects samples at four or five sites per day in the morning and returns to the SEAI office about two miles downstream from the dam, to conduct laboratory analyses of the samples. One week in the Fall, for four days in a row, Sarah noticed a grey panel van, with its windows painted over, parked in different locations near the dam and reservoir. What drew her attention was the fact that both the front and rear license plates had mud on them, which made it difficult to read the license number, while the rest of the van was clean, and also that two men with the van appeared to be filming video of the dam from different angles and taking notes. That weekend, when Sarah needed to go into the office on Saturday to finish some lab analyses, she again saw the van on a side road below the dam.

Remembering a Homeland Security training session SEAI staff had attended, Sarah thought of the "See Something, Say Something" campaign, because the activities of the men in the van seemed suspicious to her. She was able to get most of the license plate number from the van, and she called her supervisor, Ron, to report what she had observed that week. Ron told Sarah to call the Sheriff's office while he notified the security staff at the dam and the water authority manager. The van was found and stopped by law enforcement, the men were detained and questioned about their actions. Eventually, officers had enough probable cause to get search warrants, which resulted in finding maps, engineering diagrams, photographs, and videos of several dams and reservoirs from across southern California, as well as some materials that could be used to make bombs.

As Ron reviewed this incident with SEAI staff, he realized they needed to have an updated emergency plan for their facility and for all the computer data they managed. Whether there was a natural disaster or man-made one (such as an attack on critical infrastructure near their office), they needed to protect the employees and also protect their onsite data and have backups somewhere else, to be able to resume and maintain their business operations.

Security CCTV Monitoring Contractor

For cost savings and efficiency, the regional water authority has contracted with Security Video Monitoring Systems (SVMS), a local small business, to provide 24/7/365 services to install, maintain, and monitor CCTV security cameras and motion sensors at two or its dam facilities. While the onsite security staff can monitor two cameras at a time, their primary duties are physical security by patrolling around the facilities. SVMS is responsible for monitoring all the cameras and alerting onsite security of any alarms or suspicious activity.

During one evening shift, Raphael at SVMS noticed excessive 'snow' on two of camera monitors for one of the dams. When he called the onsite security staff, they reported having a clear picture for both cameras. Raphael called the field support technicians to check the network lines used for the video feeds between the facility and SVMS. They were able to determine the segment where the interference started and surveyed the cables for potential problems, where they found a splice in one cable leading to another nearby cable that did not belong to SVMS. Rather than disconnecting the splice, they installed a hidden video camera to monitor that location and hopefully see who was using the spliced connection. In addition, they notified law enforcement of the situation and dam security staff at both facilities.

There was no activity around the cable splice for three days, and no unusual activity noted at either of the dam facilities. On the fourth day, during the graveyard shift, the SVMS computer systems used for CCTV monitoring started becoming unresponsive and eventually appeared to stop functioning, which caused all the video monitors to freeze on the last viewable image. The on-duty supervisor, Stephanie, notified the dam security staff to be on alert and called her IT support staff to come in. Pursuant to security protocols, Stephanie also sent SVMS staff to the dam facilities with spare equipment to provide onsite monitoring. Powering off and restarting the systems did not solve the problem. The IT technician was able to see that the SVMS network usage was spiked at 99%-100%, which indicated a Denial of Service (DoS) type of attack was in progress. With the assistance of their network provider, they were able to determine the source IP address ranges where the attack was originating and block them from further access.

During the three hours it took to overcome the DoS attack, the SVMS systems in their office were not able to receive or record any CCTV input from any sites However, as part of their service, SVMS had installed four local digital video recorders (DVR) at each facility, which were not impacted and still recording all of the camera feeds. The local DVR data was archived and copied onto the primary SVMS servers for future reference. Because the nature of the security incident included illegal wiretapping and potential targets being the dam facilities, the FBI sent a forensics team to investigate. SVMS worked with their network provider to have additional security measures implemented to protect against DoS types of attacks, as well as being able to monitor network performance for each segment, to help detect any future wiretapping.

Prepare and Prevent

Water is one of nature's most formidable forces and anyone in the potential path of flowing water, even when it is currently restrained by a dam, levee or other retention structure, should have an emergency plan for protection of people (e.g., evacuation), property (e.g., sandbags and pumps), and important data (e.g., routine backups kept offsite). Uncontrolled release of water through dam spillways would have similar catastrophic impacts as the destruction of a dam with explosives, affording only seconds or a few minutes to get to safety, if possible.

Other events, such as hurricanes, or flooding due to torrential rain storms or rapid snow melt, offer more time to react and protect people and property; however, there still needs to be a plan in place, so people know what to do in each case. Regular emergency drills will be critical in this case. As with other types of preparation, the plan(s) should define the steps for protection of company data, including regular (at least weekly) backup of operational and other important data, with a copy stored in a secure offsite location. At least every six months, there should be a functional test to restore the backup data, to ensure it can be restored and that it is usable.

Not only should there be a company emergency operations plan, there should also be an operations plan to cover Cybersecurity functions, such as testing security policies and measures, possibly with practical drills or exercises to ensure all staff know what to do. The operational plan should include all the necessary contact information for the company's service providers (e.g., Internet services, telephone/communications services, separate network services (if applicable), application hosting, email hosting, data storage hosting, etc.).

Respond

The nature of an incident will determine what needs to be done in response. For any type of emergency situation, the protection and safety of people takes priority over everything else, whether employees, vendors, customers or visitors. Even with the best plan and regular drills, people will forget some steps and procedures during the height of an emergency, so you should follow a checklist of action items from the emergency operations plan or the computer security incident response plan.

Regular communications methods may or may not be working or available, and there should already be alternative communications procedures identified to contact law enforcement or public safety agencies, employees (who are not at the office), service providers (e.g., Internet service provider, network services, security services, etc.), vendors, and possibly customers. Based on the type and scope of incident, communications must be prioritized to address the most extreme circumstances first, followed by other matters in order of decreasing severity.

In terms of protecting and recovering your business computer systems and, more importantly, your business data (which may include confidential company or customer information), you should follow the action item checklist for cyber security incident response. Keep in mind the possible need to preserve evidence of any potential criminal activity that may have caused the incident, while stopping the spread of system damage or infiltration and minimizing business impacts. If necessary and part of emergency operations, activate business processes at another site (e.g., secondary facility or another office location).

Once the incident has been contained and there is no continuing emergency situation, take a good inventory of systems and assets, run anti-malware scans on all servers, desktops, and laptops that were connected at the time of the incident, to ensure there is no residual malware on any systems. Also check for systems or devices connected to your network that do not belong there, and remove them for possible forensic analysis. You should also try to validate the integrity of your business data and determine if any data was stolen during the incident, which may require the assistance of your data center hosting service and network service provider (if applicable).

Recover

When you have a safe work site after the emergency has ended, whether at your original office facility or at a secondary location, it's time to restore any necessary backup data that is required to restart business operations. This may not be necessary if your primary servers are hosted offsite (e.g., using cloud services) and were not damaged or corrupted during the incident; in this case, it might be possible to just setup basic replacement computers in a new, temporary office. In a serious disaster (e.g., dam collapse), full recovery may not start for several weeks and you will be operating in a temporary condition for an extended period.

Follow-up with your IT service providers, as appropriate, to ensure they are implementing necessary security measures to prevent a recurrence of the same type of cyber incident. Review and update any company policies or procedures to address any areas not already covered, that arose during the incident, and be sure to train your employees on the changes.

Defense Industrial Base

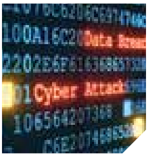
The Defense Industrial Base (DIB) sector is comprised of tens of thousands of small and medium-sized businesses which perform research and development (R&D) and provide the Department of Defense (DoD) with design, production, delivery, and maintenance of military weapons systems, subsystems, and components to meet U.S. military requirements, as well as providing incidental materials and services to the DoD.

The DIB sector provides products and services which are essential to mobilize, deploy, and sustain military operations, excluding infrastructure services such as power, water, communications, and transportation, which are normally provided by large utilities.

Techology plays a large role in most DIB business operations, including internally to the business, between a prime contractor and its subcontractors, between partnership businesses, and between the business and its vendor supply chain and distribution channels. Due to the nature of the work being performed and the products being developed, there is a high level of security required by the DoD. Beyond federal regulations and standards, many DIB businesses have their own set of rules to help maintain privacy and to protect highly sensitive data.

Examples for Defense Industrial Base:

- On-site security system with video surveillance and card access systems, often combined with offsite monitoring and alarms
- Engineering design systems for development of prototype weapons systems, subsystems or components
- Materials management systems, for ordering and tracking supplies and materials necessary for product manufacturing
- Secure email communications to receive DoD orders and respond with development status updates
- Product distribution/shipping management systems



Projects-on-Demand, Inc.

Projects-on-Demand (PoD) is a local contracting company that provides services to the DoD on a variety of technology projects. A Lead Project Manager, Rob, receives an email from someone he worked with on a DoD project about 3 years ago. There is a PDF attachment which references some statistics that project produced and the sender is asking if Rob can review it for accuracy. Rob opens the file and saves it to his hard drive so he can review it later. A few weeks later, PoD is contacted by local law enforcement that its documents have been found on a known hacker website. As soon as PoD's Information Security Response Team (ISRT) is engaged, they begin looking through network device logs and Windows logs to try and figure out what happened.

The ISRT begin to see a pattern of late night traffic on network ports 80 and 443 from three different computers on the network. As they investigate further, they notice a large amount of it coming from Rob's computer. When they speak with him, to see if he has had anything strange happening with his computer, Rob mentions the email from his old friend that he hadn't heard from in quite some time. They also see that Rob has elevated local privileges on his computer, because he is a Lead Project Manager. The ISRT asks him to call this person to verify if the email is legitimate. When Rob calls him, he finds out that his old friend did not send any email.

The ISRT pulls all three machines from the network, begins forensic scans, and finds malware hidden on all three computers. In addition, the ISRT finds attempted logins to various servers coming from Rob's account and the other two computer user accounts. Robs computer also has three unusual files (with a .rar extension) located in the Windows directory, which no one can open and that Rob knows nothing about.

In the end, all three users are asked to change passwords immediately. The three computer hard drives are imaged (copied) for future reference, then wiped clean with a low level format, and finally re-loaded with a clean image of company software. Rob has his elevated account privileges removed, because they weren't needed to perform his job. It is unknown how much data or what type of data was taken, as the .rar files found by the ISRT were encrypted and could not be opened. The ISRT did an assessment to find out what can be done differently next time and what tools are available to detect the lateral movement on their network, as well as developed policies and procedures for monitoring data leaving their network. They also switch to two-factor authentication instead of just passwords for key systems and accounts. The ISRT provided their recommended changes to company leadership for approval and implementation.

Defense Operations Contracting, LLC

A local DoD contractor, Defense Operations Contracting, has many employees who work remotely on a regular basis, accessing the network using a Virtual Private Network (VPN) client. One evening, after normal business hours, the network and security team was alerted that one of those VPN accounts belonging to a Senior Engineer was attempting to connect, but had failed the automatic posture check which verifies the remote machine has the proper certificates. The next day, the employee, Karen, was contacted by the security team and, during the conversation, Karen mentioned that when she logged in to Outlook Web Access, some of her new emails were marked as already read when she knows for sure she had not seen them yet.

The security team immediately disabled Karen's account and began looking at firewall and system logs to see if any other suspicious activity had taken place. They asked Karen if she had any strange emails or any phone calls that seemed out of the ordinary. She mentioned that she recently returned from an industry trade show she attends every year and that she was given a USB thumb drive by one of the major vendors. When she returned to work, she had used the thumb drive for copying some files she wanted to work on at home.

The security team scanned the thumb drive on a specialized computer set up for this purpose. They found some malware (malicious software) that is designed to automatically launch when the drive is plugged in to a computer, using the "autorun" feature. Upon further investigation, the malware was found to extract encoded password files from the local computer and send them to a remote server using network port 443.

In the end, the IT department purchased software which gave them the ability to allow specific "white listed" USB thumb drives and disallow others. The company now must issue approved/allowed USB thumb drives to those users who require them. The network and security teams also installed a proxy server which allows them to monitor port 443 traffic by breaking the connection and inspecting what is inside the transmission. Outlook Web Access was removed as a means to check email remotely. Finally, they issued two-factor authentication tokens to their remote users for VPN access. Now, when a user needs to connect remotely, the posture check looks for both a machine and user certificate installed on the remote computer, and the end user must log in with both their password and the temporary access number from the token.

Prepare and Prevent

Companies working as part of the Defense Industrial Base need to keep in mind they are "in a fish bowl" where a cyber incident can have far reaching consequences, not only for their business, but also for numerous other organizations, government and military as well. Practicing "Security through Anonymity" isn't enough. Recent break-ins clearly demonstrate that encryption is only part of the solution, as a great quantity of data has been stolen due to inadequate access control safeguards, policies and employee training.

Constant attention must be paid for potential information supply chain vulnerabilities, and the potential for advanced and persistent attacks from nation-state and terrorist organizations. Much of the data produced and stored can potentially have significant short and long term value, so particular care must be made to protect information through it's entire life cycle. Any "out sourcing" of services, including CAD/CAM, prototyping, testing, etc. must also be part of the IT protection program. A complete documentation management & control program must also be in place.

The DoD DFARS (Defense Federal Acquisition Regulation Supplement) subpart 204.73 applies to all companies with DoD contracts or subcontracts, and requires adequate safeguarding of controlled technical information and reporting of certain cyber-security incidents.

The DoD community has moved to embrace NIST Standards, including standards for assessment and authorization with the "Guide for Applying the Risk Management Framework to Federal Information Systems" (NIST SP 800-37r1), risk assessment including "Guide for Conducting risk Assessments" (NIST SP 800-30r1), risk management including "Managing Information Security Risk" (NIST SP 800-39), dynamic continuous monitoring practices including "Information Security Continuous Monitoring (ISCM for Federal Information Systems and Organization" (NIST SP 800-137), and "Security and Privacy Controls for Federal Information Systems and Organizations" (NIST SP 800-53r4), etc.

Implementation cyber security best practices as well as tools from the "Unified Capabilities Approved Products List" (UC APL) including "Security Information and Event Management" (SIEM) are important. Development and implementation of appropriate cyber security policies as well as recurring employee cyber security awareness & training are also important. Have a viable business continuity plan including back up and restoral, and practice it.

Respond

Proper "before the incident" preparation and close attention to Regulation / Compliance requirements can make it possible to respond to the inevitable incident appropriately. Failure to prepare can be extremely costly, lead to loss of contract, and other penalties. This is an instance were you must have required policies & procedures in place before the event, and review & practice them at least annually or when major system changes are made.

It is critical to determine how you will comply with DFARS 204.73 and NIST SP 800-53, conduct an assessment and have appropriate procedures in place.

Conduct regular training, and keep an active cyber security awareness posture across the company. Identify and train/prepare a response team, and implement your response process and procedures whenever there is a sign of an incident, as practice is key to have a competent response in critical situations.

Recover

This is one of those situations where it's best to push the pain up front. Preparation before any urgency is likely to be more comprehensive, and have the buy-in and commitment of all the necessary parties before the fact. The down side for not being prepared can have far reaching consequences. Having a business continuity/recovery plan and a trained/prepared Response Team greatly enhances the speed and confidence in recovering from an incident. It is essential to have a realistic and rehearsed recovery plan, before-hand. Some items for consideration include: restoral from backups when able/appropriate, running operations/systems at an alternate site, ultimately returning operations incrementally to your primary site starting with the least important systems & functions first, to ensure 'continuity of operations' during the transition and that the primary site is truly ready to once again handle the 'entire' operational load.

Our nation's defenders rely on business partners that supply goods and services. Not only to provide the equipment, but to help ensure safety and security is applied as an integral part of their equipment and processes. If there is a vulnerability in the chain, there is a vulnerability in an entire operation.

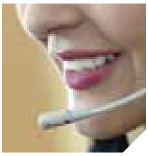
Emergency Services

The Emergency Services Critical Infrastructure sector will be depended upon heavily in the event of a disaster. Often underfunded and understaffed in normal circumstances…in a major disaster, Emergency Services resources will be under high demand and have limited ability to respond to individual needs. While 911 calls flood the emergency dispatch centers, individual, family, and business resilience preparation will make a significant difference when waiting for a delayed Emergency Services response. Some key things to think about are:

- Protect your people
- Protect your property
- Protect your business
- Protect your future

One way you can prepare yourself and your business is to perform an initial assessment – for what would you count on Emergency Services, if a disaster were taking place? What would your family and/or business need in the event of a regional disaster? Some things you could possibly do to ensure you and your business can respond in the event of an emergency:

- Communications / Call Plan – create and disseminate a call-tree with key numbers, so staff and family can be notified as to what they should do (i.e., report to work or not)
- Training – have a disaster plan and train to it for staff and family
- Community and Business Emergency Response Teams (CERT & BERT) – readiness response teams that are trained and ready to serve; join one or know who to contact



Countryside Fire/EMS Dispatch Center

Countryside Dispatch is a private organization under contract to the county and other local jurisdictions to provide emergency (9-1-1) dispatch services for fire and emergency medical response in rural county areas. Emergency calls in rural areas are routed from the county's 9-1-1 dispatch center to Countryside using automated call switching and routing systems based on the geographic location of the calling party. While Countryside uses 800 MHz radios to communicate with fire and ambulance vehicles in the field, the actual dispatch function uses a combination of radio telemetry, text paging, and computer-based call data exchange.

On a Saturday afternoon, when there is usually an increase in the number of calls, the on-duty dispatch supervisor, Carol, noticed that no calls had been received for over 30 minutes and that some of the dispatchers' computer screens seemed to have 'frozen.' Carol contacted the county dispatch center to see if they had been sending calls to Countryside and she was informed the automated calls were being sent, but not acknowledged. The county took over direct dispatch of Countryside fire and EMS crews until their system problem was resolved. A Countryside technician told Carol all the systems were up and running; however, two primary servers showed maximum memory and processor utilization, which was not allowing normal transmission and receipt of data or the use of dispatch applications. An analysis of the network activity for those servers showed a steady stream of high-volume traffic from about a dozen different external sources, indicating a "Distributed Denial of Service" attack, which overloads a system without necessarily shutting it down or damaging any data. The network technicians reconfigured their firewalls to block the unknown traffic and the servers returned to normal usage levels, allowing the backlog of transmissions from the county to flow into Countryside. Coordinating with the county, it took almost an hour to confirm that all 9-1-1 calls sent to Countryside during the potential attack on the servers, had actually been dispatched or otherwise handled. Fortunately, no lives or property were lost in Countryside's dispatch area during this time period.

After this incident, the Countryside technical support teams met with the county IT and security teams, as well as with law enforcement Cybersecurity agents. Countryside was able to change some of their network security settings to help detect this type of attack in the future and, whether the attack can be stopped or not, to send a notification to security staff before the systems become overwhelmed. An investigation is underway to find the perpetrators.

Goodhelp Ambulance Service

Goodhelp Ambulance Service is a small, private emergency medical transport company, under contract with the county to provide paramedic and EMT services in rural parts of the county. The ambulance crews have laptops with wireless connections to receive dispatch information and send patient information to hospital emergency rooms. The wireless traffic is transmitted over a Virtual Private Network (VPN) with encryption to protect the data.

Phil and Brad are two Goodhelp paramedics who were dispatched to a traffic accident. Brad noticed that the address shown in the call details on their laptop was different than what the radio dispatcher had given. They responded to the radio dispatch location, found the accident and starting treating the injured victim. On their way to the hospital, they radioed their estimated arrival time and said they had sent the patient data via the laptop. The hospital told them the patient data was not received, so they used a secure radio channel to provide the information. When they had dropped of the patient at the emergency room and returned to the Goodhelp office, they reported the laptop problems to the IT support team.

When the laptop was examined, the technicians found malware that redirected wireless data, sent to or from the laptop, to an unknown server that then sent false data to the laptop. The technicians were able to remove the malware and restore the laptop to its proper, secure communications. When questioned, Brad told them he had been working on a document on his home computer, copied it onto a USB drive, and then copied onto the laptop to finish the document at work. He said he also noticed some odd behavior in his home wireless connection, but didn't think much about it. The technicians were able to find the malware on the USB drive and remove it, and told Brad how to clean it from his home computer. Goodhelp implemented a policy, along with system security settings, which prohibit the use of USB drives on their laptops.

Prepare and Prevent

To prepare your family and your business to handle medical emergencies, look into getting them certified in basic first aid and emergency response ahead of time. Consider the Red Cross for classes and certifications in First Aid, CPR, and defibrillation. If there is a regional disaster, food and water can be in short supply. If the event goes on for an extended period of time, be prepared by having provisions such as food and potable water available for your family and for your employee's if you must keep your business open. Be prepared and have first aid kits available and have batteries and radios on hand so you're able to tune in and receive information about the local and regional emergency response gathering places. The disaster response teams at these centers can get you quicker medical attention than if you call for help from your business on the standard 911 line that will be most likely be inundated with requests for help.

To prepare your family and businesses to handle a fire emergency think “Safety First.” Before a disaster strikes, survey your business to establish a safety baseline. Identify all potential areas of risk or danger including power, water, fuel sources (propane, gas, etc.) and potential physical dangers such as glass and thin metals that could become dangerous following a disaster. Define a safe, default gathering place for your employees to meet in the case of an emergency. After a disaster strikes, survey your immediate surroundings for potential hazards, look for immediate dangers such as exposed electrical, sharp metal and broken glass and leaking fuels. Move to your designated safe place – be sure it is still safe after disaster strikes; if it is unsafe, move to a secondary location and ensure all of your people are informed and accounted for.

The final part of Prepare and Prevent for your business deals with Law Enforcement. Inform and train your people of the human dangers during a disaster. There are those people who will take full advantage of the situation and put your people and your business at risk, physically. In preparation for your business’ response to an emergency, develop your internal BERT plan. From a cyber disaster perspective, make a policy for your employees so they know what prioritized actions they need to take following a regional disaster, some ideas may be:

- Get my businesses computer systems back on line as fast as possible.
- Have capabilities in place to make sure I don’t propagate the problem that caused the incident in the first place as I come back on line.
- When I’m clear (i.e., malware removed), re-engage with my customers and my suppliers.
- Ensure I have not lost any of my data, complete the backup of my business’ crucial files and ensure they are available; use existing backup files to restore any lost or damaged data
- Designate who to contact, including how to engage law enforcement, when staff discover what appears to be a data breach

Respond

In the event of a regional disaster or a regional cyber-event businesses should look to protect what they have in place and activate their Business Emergency Response Team (BERT) program. Some issues and questions a business would look at would be:

- Do you disconnect your systems? (Sometimes, you first want to capture a remote location where data is being sent.)
- Do you power down your systems? (What is the operational impact and what happens when they are turned on again?)
- What other actions do you take or not take to protect your data and equipment? (If you have contacted law enforcement, follow their directions.)

- Perform an assessment of your IT environment and determine the best way forward for your company. The answer may be different for different parts of your IT infrastructure.

Recover

After a regional disaster or cyber-event, businesses will want to ensure their business networks are capable of handling their client's data and the network can return to business as usual. Businesses will want to access and possibly install their data backups, verify their important software/hardware configurations, and validate their clients' data.

It is at this time, based on the assessment of your IT environment, you would incrementally reinstate your businesses IT network in accordance to your BERT's recovery plan. If you have complex software or hardware configurations you will probably have stored these configurations online or in some remote location.

The configurations will need to be retrieved, verified as still accurate for your current network environment and installed with periodic testing to ensure the settings have not been corrupted. It is also critical to ensure that you have located and resolved the cause of the incident before you reconnect with clients – you don't want to cause a recurrence of the event. After installation of your business networks configuration files it is time to restore your clients backed up data, however again as before, you will need to test this data to ensure you have no corrupted files.

One last important note: if you are recovering your business after a significant cyber event, it is important that you know how your network operates in a normal business environment. Have you ever established a network baseline? Do you know or are you familiar with how your businesses network operates so you can identify if things are not operating correctly. If you are unfamiliar with how your business' IT network operates and you are unable to identify if it is not working correctly, you may need to work with a professional company to assist you in restoring your businesses network and its data.

Fraudulent websites and servers used in attacks more than tripled since 2012. More than 50% of the total number of individual targets were fake copies of the websites of banks and financial organizations.

Financial Services

Many businesses are operating on a very small margin, where an error or fault in the banking or financial systems can potentially have a high impact or even disastrous consequences on a business. Financial loss can trigger an impact through every aspect of an operation and associated businesses. Purchasing, inventory and even sales may feel the crunch.

Internal staff are likely to be upset or may even abandon a business when payrolls are delayed. Financial disruption can be profound and it may be very difficult to restore not only the business, but the business' reputation as well. In the case of a financial institution data breach, where client and account information is compromised, the foundation of the establishment is rocked and competition may gain a large advantage to win customers over to their institution.

Examples for Financial Services:

- Accepting payments/deposits *(cash, checks, credit cards, EFT)*
- Security system and safe for protection of money/valuables
- Armored transport vehicles
- ATM machines
- Online banking
- Locations to cash checks

Marti's Floral Shop

Marti Clark owns and operates a floral shop. She handles their transactions, payroll and other banking online through a third-party organization. Driving to the shop one Monday morning, Marti heard on the radio that their branch bank had been breached. When she arrived at the shop and tried to access her account, everything was frozen. She called her customer service representative and after a long wait, someone finally answered the phone. They told her that they experienced an internal "issue" and they would be notifying affected customers as soon as they had verified information. Her representative also shared that he was not sure what information, if any was in jeopardy. When Marti asked why she seemed to be locked out of her account, they explained that all functions and services would probably be blocked for a week, at minimum. Marti panicked fearing the worst. What was she to do?

Banking Institution

In a recent news story, a nationwide bank reported that an employee with access to account-holder information allegedly leaked personally identifiable information including names, addresses, Social Security numbers, phone numbers, bank account numbers, driver's license numbers, birth dates, e-mail addresses, family names, PINs and account balances to a ring of criminals. With that information, the fraudsters reportedly hijacked e-mail addresses, cell phone numbers and more, while keeping consumers in the dark about new accounts and checks that had been ordered in their names.

Hundreds of customers in the U.S. Western states reportedly had their accounts hit, and numerous suspects linked to the breach were arrested by the Secret Service.

The fraud, detected by the banking institution nearly a year ago, is just now notifying affected customers of the breach. What can the affected customers do? To start with, you can get helpful information about identity theft from the Identity Theft Resource Center (http://www.idtheftcenter.org/), or from the FTC (https://www.identitytheft.gov/).

Prepare and Prevent

An extremely important measure for any business to take is to keep local copies and records of any important financial data. When systems fail and data is lost, proof of balances and content of accounts can save businesses money. Beyond that, a business should have a plan for continuing operations without their normal means of banking. Consider a secondary account as backup if only your primary system is affected. Keep cash and valuables in a manual safe and use cash to make sales when electronic transactions are not possible. If feasible for your business, keep extra inventory on location to continue making sales when you cannot pay a supplier. Consider keeping a credit card imprinter as well.
If the situation is drastic, you may need to prepare to use a barter system for essentials.

Respond

When an incident occurs, determine what the entire situation entails. Figure out the severity, amount of damage, and estimated time of recovery. As applicable, notify authorities, legal assistance, and/or your insurance company. If you have clients that should be aware of the situation, let them know as well. There is a breach law in California that requires customer notification. (See resources and reference to SB24) Ensure that your emergency cash, cards, and valuables are secure. Continue to keep physical records of all transactions and business operations. If you suspect that your computers or network are at risk of a breach, disconnect them.

Recover

Make sure that your accounts are stable, safe, and functional before returning to use them for financial processes. Continue manual operations as you verify the accuracy of the accounts, using offline data to make sure nothing is missing or incorrect. Update your accounts by capturing the data from the time spent offline. Do your best to reach out and re-establish the connections with clients that you may have lost. Above all, verify that you comply with all legal policies and complete any duties such as reporting. If the situation is a long-term disaster, figure out where you can obtain cash and begin to use bartering as necessary.

"For the second year, the food and beverage industry made up the highest percentage of investigations at nearly 44%."

-Trustwave Global Security Report 2012

Food and Agriculture

Over the past century the U.S. has slowly moved from an agrarian-based society through the industrial age and is now well ensconced in the information age. As of 2011, most farming and food production is relegated to "corporate farms" and the family farms of yesteryear are all but gone. Supply chains from growers through merchandisers to local stores include a key information network that relies on instant and accurate data flow. Not only does our food "network" now involve the timing and readiness of the actual products and distribution of them, but it also includes digital connectivity between growers, suppliers, purchasers, distributors and the actual point of sale as well.

From the field to the table, Information Technology has a profound effect on our Agriculture and Food production and delivery.

Examples for Food and Agriculture:

- Online ordering from suppliers and shipping with distributors
- Automated food storage/preservation system *(refrigeration)*
- Computer-based inventory management and accounting systems

Restauranteur

Pete Smith owns and operates an upscale, fine-dining establishment in downtown San Diego. He hopes to build his brand and expand in the next six months. Recently he has noticed that some of his most prized customers were not making reservations as often as they used to for dinner. He had expanded his staff with experienced servers in anticipation of the new facility, but, with the drop in business he was now concerned. His menu was the same; he had extended his hours and even added a web page to make it easier for his customers to book a reservation. What was the challenge? What happened?

Pete's new web page was beautiful, but, in fact, the reservation system had been hijacked. His choice customers had actually been making the reservations but no longer were receiving their confirmations and moved on thinking Pete's place was in trouble since they did not hear back from him. Phone calls and a proactive e-mail campaign soon rectified the situation. Pete learned to regularly check his promotional channels and back-end technology.

Grocery Merchandiser

Ken Lawler is the lead merchandiser for a major grocery-chain. He is responsible for the daily supply of fresh produce for his company's stores across the nation. He was hard at work one morning, checking in with his suppliers, when he experienced a strange behavior from his computer. Pop-up windows start appearing every few minutes on his screen. He closed them out each time, but they were persistent. He stepped away from his desk and got a cup of coffee from the break room only to hear other merchandisers experiencing the same challenge. When the team arrived back at their desks to continue their mission, all screens had the same message on them – "out of service." As the lead merchandiser, Ken picked up the phone and called the head of IT. They too, had noticed strange behavior in the network and were tracking things. However, things went from bad to worse. They had no access and buying/supplying has screeched to a halt. The impact – with only an hour outage, the window of opportunity closed and their stores across the nation did not have fresh produce for several days - some even longer, depending on how quickly the IT folks were able to rectify the situation.

A discovery process later revealed that one of the team members had taken a spreadsheet home to work on it the day before via a thumb drive. Their home computer's anti-malware was out of date and the machine was infected. Once inserted, the thumb drive also became infected and in turn it infected the company's network. This was an innocent, but costly challenge for the company. Ken and his IT department established an IT policy for their staff and installed end-point security including device scanning upon insertion.

Prepare and Prevent

Resiliency begins with planning, policies and preparation. In both of the previous scenarios it is evident that there may have been a lapse in these key areas. If your staff is not up to date on your policies and procedures, or forgets to regularly check systems and prepare for an unexpected disruption in services, the impact can be great. A written plan with associated policies and procedures in addition to an educated staff can save not only money but also perhaps your business.

Consider part of the planning process to look at your business life cycle and key dependencies. You should also build alternative sources and relationships so they are at the ready should it become prudent or necessary.

Respond

In a disaster, whether it is natural, man-made, physical or cyber, first responders say your planning is the key component for survival. Assessing damage and calculations to minimize losses are the first steps. An educated team that can execute to a plan mitigates loss and in some cases allows for a short-term rollover to redundant systems and perhaps even continuation of services through alternative sources.

Recover

In the area of data loss, the SBA cites that, in 2010, 70% of SMBs who experience major data loss fail within one-year after that loss. Protection for one of your greatest assets – data – should be foundational to your business. Again, in today's Information Age, there are few businesses that do not have a cyber or online component that is instrumental to their business. A data backup and recovery plan must be included in your overall planning process. For the immediate circumstances be prepared to engage alternative resources.

Government Facilities (Education)

The national Government Facilities Sector includes federal, state, local, and tribal government buildings and other facilities located across the country and overseas. These government facilities provide a wide variety of services to the public and businesses for personal, commercial or recreational activities. Other government facilities are closed to the public, because they contain highly sensitive or confidential information, materials, equipment or processes. The facilities include general office buildings, courthouses, legislative buildings, embassies, national laboratories, and special military installations.

There is a subsector for Education Facilities, which includes both publicly and privately owned facilities for pre-Kindergarten through 12th grade schools, community colleges, institutions of higher education (universities and colleges), and trade schools. In addition, there is a subsector for National Monuments and Icons, which encompasses a diverse array of assets, networks, systems, and functions located throughout the United States.

Examples for Government Facilities:

- Development/Construction Permit Processing
- Public Water/Sewer Utilities Payment System
- Student Registration System
- Government Personnel Management System
- Protected Wilderness Access Permit System

ACME House Builders, Inc.

Alison was nearly done completing the third out of four online permit applications for her constructions company, ACME House Builders, to demolish and rebuild four houses in a residential area of east San Diego, as part of a regional redevelopment project. On that Thursday morning, when Alison clicked on the link to go to the next page, nothing happened; even after waiting for a few minutes, the page never changed. Alison called the development agency's help number and, after being on hold for several minutes, she was told that the permit system had stopped functioning and they were working to get it back online. She was also told that any pending transactions were probably lost and would have to be re-entered, or she could come into the office to fill out paper forms and pay the applicable fees.

Two hours later, Alison tried to access the development agency's website to check the status of pending permit applications, but got an error message that the site address was not available or didn't exist. As she tried to access other pages on the agency's website, they all had the same error message. Since they didn't want to delay getting the permits, Alison sent Curtis, one of the project managers, to the development agency office to complete the paper forms. She told him to be sure they didn't get double-charged fees for any of the permits, since some were completed online before the website problems.

When Curtis returned a few hours later, he told Alison that the agency's website had apparently been the target of a cyber attack, called Denial of Service, which overloaded the server with useless network traffic and didn't allow the system to function and process legitimate transactions. None of Alison's earlier permit applications were actually processed. Fortunately, the attack didn't affect the agency's internal network or systems, so they were able to continue processing permits in the office. Curtis was able to verify the correct fees were charged and paid for each permit, without any duplication.

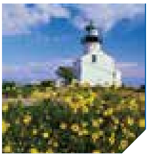
Party Hearty Event Managers, LLC

Elizabeth and her husband, Stan, own and operate a small business, Party Hearty Event Managers, which creates and provides special events for local companies, which often includes obtaining permits for public venues. One Thursday afternoon, during a team-building event for managers at a regional retail company, occurring in a portion of a large public park, Liz was contacted by a police officer who said he received a complaint that the event did not have the proper permits.

Liz advised the officer they had all the permits and tried using her mobile phone application to access the permit system, but she got an error message that the system was not available, so she asked Stan to get the printed copies. In the meantime, the officer tried to access the online permit system from his car computer, and he also got an error that the system was not available. Stan provided the printed copies of the permits for the team-building event, so the officer was able to close the complaint and leave to handle other calls.

Liz called her office and found out the staff had been trying to apply for permits all morning, but the agency's permitting system was not available and they were not able to check the status of pending permits or get copies of issued permits. Stan and Liz had to figure out what to do about obtaining permits for several upcoming events, since they had only used the automated, online system and weren't familiar with any manual process, and they didn't know how long the online system would be unavailable. Late in the afternoon, one of the staff members called Liz to tell her the online permit system was available again, and the agency was telling customers that they had been the victim of a Denial of Service (DoS) cyber attack.

Back in the office the next day, Liz and Stan met with their small staff to discuss the necessary procedures for permit applications in case the online system was not available again in the future. They also clarified the internal procedure to always print copies of approved permits and have them onsite at each event. After the staff meeting, Liz and Stan had a conference call with one of the business managers and the IT manager from the public permitting agency to ensure that none of Party Hearty's private information had been compromised. They were assured that the cyber attack only stopped normal operations of their internet-based systems and that no data was breached.



Higher-Ed National Tours Corp.

After retiring from 25 years in public service, Frank started a small business, Higher-Ed National Tours Corp., to teach college students about preservation, management, and maintenance of national monuments, national parks, and state or local historic landmarks. Frank has contracted with several local universities to provide tours of national monuments across the southwest United States and to conduct seminars regarding their history and management, as part of college degrees in Public Administration, Recreation Management, History, Environmental Sustainability, and similar majors. Frank provides a combination of classroom and online lectures, plus onsite tours as part of his contract services.

Part of Frank's contracts include non-disclosure agreements (NDAs) and the ability for Frank to login remotely from his office into class enrollment systems for five large universities. This allows Frank to directly obtain student names, ID numbers, email address, phone number, degree major, course number/title, instructor's name and phone, school term/session, and other administrative information (i.e., student emergency contacts). A separate notification is provided for any students with disabilities or impairments who need special accommodations. Frank uses the information to manage both his lectures and tours, with the capability to notify the students of pertinent information.

In addition, Frank has login access to an online permitting system, hosted by the state, that covers many of the regional parks and monuments. Frank uses this system to request permits for the various classes, and it allows him to enter some basic student information, so the state can track attendance at the sites. It also allows Frank to view permit approval status, print approved permits, make changes to dates, times or attendees, or to cancel a permit.

On a Monday afternoon in the Fall, three of the universities contacted Frank to inform him he had violated his contract and remote login rights, by trying to access restricted data over the weekend. Frank told each university contract liaison officer that he had been in the hospital since Friday morning and was just released at lunchtime to go home for bed rest, and that he had not used his computer for remote access to their data since the prior Monday. Frank was able to convince the three schools to work jointly with him to investigate what appeared to be a targeted cyber attack against them using Frank's computer (without his knowledge). Because the related incidents involved two state colleges and one private college with campuses in several states, the regional Law Enforcement Coordination Center was notified and sent a computer forensics investigator to Frank's office.

The universities' IT security teams determined that their protective and control measures were able to stop any unauthorized access to restricted information. However, all of the student and instructor data, to which Frank has authorized access, was exposed and probably compromised, so the schools initiated their procedures for data breach notifications. A forensic analysis of Frank's office computer revealed a Trojan horse program had been installed, which opened a "backdoor" for remote access into the computer; along with a key logger, which captured all the keyboard activity and provided the attacker with all of the information necessary to login to each of the university systems.

An FBI agent told Frank that is has become a common tactic for cyber criminals to attack small businesses, which tend to have less security measures, and use them to gain access to larger targets. Frank's hard drive was removed and impounded as evidence, so Frank got a new system and made sure it had the recommended security tools. In addition, the universities changed their remote login procedures to now include the use of a physical security token in combination with a User ID and password, so capturing keystrokes would not provide valid login credentials.

Prepare and Prevent

An organization with a "dot-Gov" domain, or those government agencies with a dot-com or dot-org domain, are obvious targets and constantly being probed by cyber criminals and others for vulnerabilities – with somewhat frequent success, based on the number of government systems that are in the news for being hacked. Even with millions of dollars going toward Cybersecurity, it's still not a matter of "if," but a matter of "when" an attack will succeed. Because many government agencies do have Cybersecurity resources which make it harder for those attacks, cyber criminals turn to SMBs which may have connections with government agencies, because they don't usually have many security measures.

So, if your business is a supplier, vendor or contractor with a government agency, you will have one set of security issues to address. If your business depends on the government as a customer of their services, you will have a different set of security issues.

First, for those businesses which contract in some manner to provide supplies or services to a government agency, your operating procedures, security plans, and emergency plans need to take that business relationship into account. Many government agencies now offer or provide access into some of their systems for the SMB to interact with them electronically, which may include order processing, product shipping and delivery, billing, payment, contract or project management, and exchange of customer information (e.g., the SMB provides contract services to the agency's constituents). Some agencies will require the SMB to provide a minimum level of security measures and system controls for their own systems, and certify they are maintained correctly, in order to be allowed access to the agency's system. Sometimes that minimum level might not be sufficient to adequately protect the SMB's systems, and the business should perform a risk-based threat analysis to ensure they have the necessary security measures in place, beyond any stated minimum. If possible, the network connection between the SMB and government agency should be separate from the SMB's internal business network, which can be accomplished by using a router-based firewall to segregate sub-networks.

As with other industry sectors, preparation includes making regular backups of company data, storing one copy onsite In a secure place) for easy retrieval and storing one copy offsite in a secure location for business continuity and disaster recovery purposes. At least annually, perform a test recovery of backup data to check its integrity and ensure it is usable.

Second, for those SMBs which rely on government agencies to provide online or otherwise automated services for their business operations, your operating procedures and emergency plans should take this into account. There should be contingency plans for switching from automated processes to using manual procedures in cases where the government agency's systems are not available. The SMB still needs to have its own security plan and incident response plan, and to ensure its own systems are adequately protected with proper security measures, but not for contract compliance reasons.

Respond

No matter what kind of relationship a SMB has with a government agency, when a cyber incident is discovered, the SMB must take action. Response activities will be virtually the same, except communications with the agency will vary depending on the business relationship.

Prevent spread of the incident by quarantining affected systems or, as another approach, allow the impacted systems to remain operational and segregate all other systems (i.e., behind firewalls or other defensive measures) to protect them from the infected systems. Be prepared to capture, and save in a secure location, log files from impacted systems, security monitoring systems, and other sources which may have tracked the start of the incident. Once the incident has been contained, check all systems that don't appear to be impacted to ensure there is no malware on them (including rootkits or backdoors), and also to ensure any data stored on them is still intact and not corrupted or missing. Those systems deemed to be "clean" may be returned to normal operations, as long as the network has also been secured to prevent another attack or re-infection.

Start reviewing log files to determine the source and nature of the attack. Collect and preserve any hardware or software that may be needed as evidence or for insurance claims. Begin notifying suppliers, vendors, distributors, and the government agency (if applicable) about your situation and when you think operations may return to normal. Implement manual procedures until systems are cleared for operation, and keep documentation of any actions which will need to be entered into a system after they are restored. Start the process of retrieving backup data from the secure onsite or offsite location, to prepare for restoring the data. If company data was breached and potential extracted, including data related to employees, business partners, customers or contract agencies, take necessary steps to prepare for any required breach notifications. Also start preparing any press releases or other external communications that the business will want to release regarding the incident (be sure to include your legal counsel in this process).

Recover

As stated elsewhere, having good planning, preparation, and response plans, and following them, does not guarantee a successful recovery, but it places the business in a much better position to return to normal operations after a cyber incident or other emergency. One of the initial stages of recovery involves taking inventory of your physical and digital assets, to determine their condition and fitness for continued use. If hard drives or other equipment must be impounded as evidence, new hardware will be required, as well as replacing (reinstalling) the associated software for those systems, and restoring any related backup data to the new systems. In addition, enter any business transactions from the temporary, manual processes that will be necessary to fill the gap from system downtime.

Continue any manual operations until all necessary systems are back online and functioning normally. Notify your suppliers, vendors, distributors, customers, and government agency (if applicable) when you are ready to make that transition back to automated processes. Provide any required incident documentation to the government agency (if applicable) and to your legal department and law enforcement, as appropriate.

Many organizations and individuals look to the government for all forms of protection. Cyber security is specifically a shared responsibility. Businesses must take the first step to educate their staff, if they truly wish to become cyber secure. A cyber attack on our national infrastructure could totally disrupt our economy and way of life. Are you prepared?

Healthcare and Public Health

People will value their health over money. This simple fact makes protection of Healthcare and Public Health Critical Infrastructure sector extremely important. Otherwise, there is so much to lose. Collectively, this sector of our national critical infrastructure represents an immeasurable investment and is of tremendous value to us as individuals, equating to value across our nation and around the world. Healthcare organizations must demonstrate security controls and quality business practices in line with the risk they face as they conduct daily business protecting human life. This is important because Public Health Critical infrastructure is an appealing target for Cyber Criminals.

Security breaches are being used to hold organizations hostage against hefty fines for regulatory violations. Medical insurance identities are being stolen and sold so that uninsured people can assume the identity of a covered individual. Criminals are inventing new ways to exploit this sector every day. Theft of Personal Healthcare Information (PHI) is being used to obtain medical treatment, supplies, and equipment which are then attributed to the victim and can have potentially fatal results if incorrect medications or treatments are administered.

Examples for Healthcare and Public Health:

- Physicians' Online Prescription System with Direct Link to Patient's Pharmacy
- Hospital Surgical System for Non-Resident Surgeons
- Regional Public Health Services Systems for tracking infectious diseases

Dr. Donna Smith, MD – Family Practice

Dr. Smith is part-owner of a family practice located in a beach community in San Diego, California. The practice has three physicians, ten nurses and other support staff. The community has a large population of non-native San Diegans and a large number of tourists that visit this community each year. Dr. Smith and her partners have recently implemented an Electronic Medical Records (EMR) system to help manage patient data, improve referrals with area hospitals, and improve billing accuracy and efficiency. Dr. Smith also subscribes to EMR's "Software as a Service" (SaaS) offering and relies on her personal email and file server to conduct daily business operations. One day while performing a routine examination, the San Diego region suffered a power outage. It was a major outage that was expected to last for more than a day. Dr. Smith's staff knew what to do because, about a year ago, they participated in a table top exercise with other critical infrastructure sector participants. The doctor, her partners and patients were all safe.

ABC Pharmacy

Henry Donner went to the local ABC Pharmacy to pick up a prescription that his doctor ordered. He was waiting in line to submit his prescription. As Henry stood in line he observed a man hovering around the isle near the pharmacy counter. He felt a bit uncomfortable. The man appeared to be homeless or in a very bad way. He had tattered clothes and was unshaven with matted hair. He just kept pacing as though he needed to talk to the pharmacist but didn't want to wait in line like everyone else. Henry thought he would give his position to the "homeless" man and help him out. The man started ranting and distracted everyone in the pharmacy. Another man, a few people in line behind Henry rushed up to the desk and said "I can help." He appeared to rest his hands on the desk and motioned to the man to come with him. As fast as it started, the two men walked off and the patrons began whispering about how strange the whole thing was. Henry proceeded to provide the pharmacist with his paper prescription, and then wait in the second line to pick up his pills.

About six hours later, the same two men came back into the pharmacy, and the same "drill" was repeated – the pacing, the distraction and the escort out the door. The pharmacist got a very strange feeling in her stomach and asked the store manager to review the video tape to see if it was actually the same two men from earlier in the day again. After reviewing the tapes and zooming in on the scene, they noticed the man standing in line behind Henry actually appeared to have done something to the pharmacy computer. With a tight zoom they saw his hand swiftly place a thumb drive in the back slot on the computer, and the same man removed it about 6 hours later! They were dumbfounded. Why would he do that? Well, they discovered later he had put a keylogger on the computer and now had access to all of the pharmacy's and customers' information. This was a serious breach and one that required immediate action.

This breach could have been prevented by simply setting the operating system to not accept any removable media connections through the USB ports, or at a minimum, physically blocking the ports.

Prepare and Prevent

Conducting a risk assessment on your IT system and its support devices will enable you to view the risks your network and its data face, and options you have to remediate them. Annually reviewing this assessment will enable you to update your assessment and make changes to ensure you stay protected. One option may be to have a data loss recovery plan; this plan can be one of the first steps to rebound from an incident. Part of this plan can be to establish an offsite backup site or subscribe to an offsite backup service. This can help ensure your data can be restored in the event of a failure. Also, consider physical security at the same time you are tightening your Cybersecurity. What could Dr. Smith's staff do to better prepare and prevent their office?

Since Dr. Smith must be compliant with HIPAA, she has hired a 3rd party contractor to perform a risk assessment of her IT systems. Dr. Smith's IT provider performed an assessment of her IT risks including taking into account technology, human life and public health risks. Her organization's risk-based-assessment concluded that her biggest risks were:

- Security of the facility containing health records – her office
- Security (hardening and patching) of her e-mail and file servers
- Physical Security of the computers in her office

In response to these risks, Dr. Smith worked with her IT provider to improve her security in ways that also gave her more business value. These included:

- Replacing her office's server (originally located in the closet) with an "Infrastructure as a Service" (IaaS) product provided by a Good Informatics Practices (GIP) qualified cloud provider which hosts e-mail and medical files in a secure cloud offsite from her facility. These servers are at the IaaS Provider's datacenter, where they are contracted to be secure, up-to-date on their patches and would be protected from power outages with a secure rack mounted Uninterruptable Power Supply (UPS).
- Another way to reduce her risk would be to use a "Software as a Service" (SaaS) product for encrypting and managing her e-mail in the cloud, thus enabling her to share medical records securely via e-mail.

- The last risk control she could put in place would be to install desktop encryption software on her office PCs, this would provide another layer of security protecting her patients data that is stored in her offices PC's from such risks as theft, fire, flood, etc.

Together, these actions are simple steps that allow Dr. Smith to reduce her company's IT risk significantly and provide her business with a significant new business tool; securely storing and sharing her patients medical records.

Respond

When you suspect something might be wrong, trust your "inner voice" and check. Dismissing things that feel wrong can actually allow major incidents to occur un-noticed. If you have planned well, you and your teams will know what each person should do if an incident happens. Again, let's look at Dr. Smith's response to her incident.

Dr. Smith calmly ends her exam. She still has Internet and server functions for a few minutes and she quickly assesses through the Internet that this is a major outage. She enacts emergency shutdown of the computers in her office, locks the office and leaves the premises. However, her work is not done.

Dr. Smith enacts her Business Continuity Plan and makes sure she and her family has water and they are secure. Then, she begins to coordinate with her affiliated local hospitals.

Since she implemented a secure cloud service to protect her assets, she is able to access her e-mail and EMR's datacenter so her patient's medical files are available. She has a few elderly and chronic patients that she feels are at risk during the power outage. She accesses the EMR program and is able to send those records securely to hospitals using her new (IaaS) encrypted e-mail service so those files are now ready should a crisis arise.

As the disaster progresses, health problems arise with tourists who are stranded and can't get home. Simple things such as medications and first aid become important in the community. Again, her preparedness pays off. Using her EMR software system, she is able to receive medical records from doctors outside the region, since it is stored in a datacenter rather than within the geographical location of this event. She has immediate access and is able to assist doctors who must help their stranded patients.

Recover

In both cases, quick thinking and a solid plan helped avoid an extensive recovery time. While both incidents show the potential for loss of reputation and potential business, it did not become an issue in these incidents. Again, in the case of Dr. Smith we see the power is restored. Dr. Smith returns to work and resumes business as if nothing happened. Her choices to use a secure cloud environment allow her to power up her office computers and confirm with her IT Provider that everything is functioning correctly and she has not lost any of her patient's data.

The future of health-care, medical devices, pharmaceuticals and genomics are increasingly digitally interdependent and demand good informatics practices. To that end, for the protection of the patient and providers, good informatics practices must be implemented now and throughout the future.

ENDING
1 2 3 4 5 6 7 8 9 10 11 12
13 14 15 16 17 18 19 20 21 22 23 24
ADSL
ADSL
ADSL
ADSL
ADSL
ASC1024
ADSL
ANNEX A
26AWG 771 COPARTNER
ADSL
ANNEX A
ASC102
ADSL SPLITTER CARD
ANNEX A
1024
ADSL SPLITTER

Information Technology

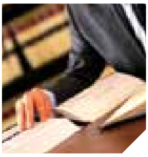
Information Technology (IT) is a critical infrastructure (CI) for almost all businesses and most families today, as it is the core means of conducting business and engaging in social activities across the world using the Internet and corporate networks. In addition, most, if not all, of the other critical infrastructure sectors rely not only on the Energy Sector, but also on IT for their underlying infrastructure; therefore, disruptions in service or attacks against these sectors will have negative impacts to the other sectors.

IT service providers are a fundamental backbone of critical infrastructure. Some of the concerns for IT companies include malware proliferation, denial of service attacks or other service interruptions, and compromise of client data.

Examples for Information Technology:

- Internet Service Providers (includes some Cable TV, Satellite TV, and Telecommunications companies)
- Data Center Services
- Local or Wide Area Network Services
- Cloud Services (storage, applications, etc.)
- Software as a Service (SaaS)

Businesses in Acton



Small Law Firm

Tom Atkinson is a partner in a small San Diego law firm that specializes in U.S. patent law, and because he has some technical background, Tom helps manage and monitor the firm's computer systems and applications. The firm keeps information about each of its clients in its company database, including detailed contact information, and tracks the progress of the patent filings, but they do not have any of the clients' confidential trade secret information in their files. Tom maintains the firm's website with information about its services, which also includes an online contact form to request information from the firm. The online contact request information, which is only saved for 24 hours on the web server, is sent via e-mail to the company e-mail account, where it is reviewed by office staff and routed to the appropriate legal staff for response.

One morning, the company's Internet Service Provider (ISP) notified Tom that it was monitoring unusually heavy network traffic on their company servers. Tom also found that their website contact form had been modified and that some of the client database was corrupted. Tom worked with the service provider to shut down access to their company servers, except for the system administrators. The ISP security team reviewed server and network activity logs for the 24 hours prior to the unusual activity and was able to find that someone had hacked into the company's website and changed the online contact form to route the data to a different server, somewhere in Asia. The ISP security team also determined that it appeared most of the client database had been exported, also to a server in Asia. The system administrators were able to remove the malicious software and restore both the website and the client database. They also made configuration changes to increase the security of both systems, including further segregation of the database server from the web server through another, internal firewall. Tom was thankful their contract with the ISP included system backups, data restoration, and security services. A year earlier, before the new ISP service, Tom's company would have had to recreate the website from scratch and manually rebuild their client database from paper records.

Tom sent notifications to the firm's clients to inform them of the potential breach of their contact data and to be watching for possible cyber attacks, as well as the possibility of identity theft. Tom also notified local law enforcement and the FBI of their breach. The following week, Tom was contacted by three of their clients, all of which were in the biotech industry, that there had been unsuccessful attempts to attack their respective corporate systems. At this point, with his clients' permission and cooperation, Tom contacted the FBI to inform them of the additional attempted attacks.

Internet Service Provider & Data Center Provider

Carol Johnson works as a network administrator for a small Internet Service Provider (ISP) in Colorado, which provides services to small business clients across the western United States. Some of her clients are hospitals and financial institutions. In addition to having network equipment at their headquarters facility, her ISP firm has its equipment hosted in several data centers and telecommunications centers in four western states, including in southern California. One day, Carol was performing routine security checks when she discovered a configuration anomaly in her Domain Name System (DNS) servers located in California.

[Note: DNS is an Internet service that converts user-friendly domain names into the numerical Internet Protocol (IP) addresses that computers use to talk to each other. DNS and DNS Servers are critical components of the overall network infrastructure and of each computer's operating environment - without them, you would not be able to access websites, send e-mail or use any other Internet services.]

Upon further investigation, Carol discovered that her clients' inquiries were being redirected to rogue servers in Asia. Criminals had hijacked Carol's DNS servers, and could control what sites her clients connected to on the Internet. By controlling DNS, criminals were able to divert her customers to a fraudulent website that infected computers with malicious software (malware) which in turn prevented them from connecting to legitimate websites. Carol's team began notifying all their clients to cease any data entry and worked with their clients to remove the malware until the problem was resolved.

Carol contacted the data center hosting facility's security team and notified them of the situation. They advised her that one of their facility firewalls had been breached a few hours earlier and some web servers in the facility were found to be infected with malware. They fixed the firewall vulnerability and added her DNS servers to the list of impacted systems, then continued a systematic review of all other network devices in the facility. Since the facility uses several commercial network service providers for their many customers, they sent notifications to the various security teams and customer support centers to be on the alert for the particular system files and configuration changes that resulted from the malware. Following approved security operations protocols, appropriate law enforcement agencies were notified. Infected systems were cleaned and backups were restored so that services could be reestablished. Once Carol's DNS servers were brought back online, her clients were able to start using the Internet again.

Small Medical Practice Office

It was a typical day at the North County Pediatrics Office. The office had been packed all day long with patients but the staff was doing a fantastic job of keeping up with the flow of families and children. The waiting room was full of patients who had regularly scheduled checkups and several children who were under the weather. Doctors Debby Graham and Steve Jennings own the North County Pediatrics practice and a three person support staff supported them this particular day. Debby and Steve had a slight break in patient visits and reflected on recent changes they had made to their practice.

Over the past several months, the practice had adjusted their business practices and tools to minimize the impact of the loss of Internet connectivity. The practice had expanded their patient tracking application to include a back-up capability in-house and hosted it on an onsite server. It had previously been hosted solely by a reputable third-party hosting service but the loss of Internet connectivity on multiple occasions had impacted the practices ability to service their patients. The practice had also leased a new merchant terminal to take credit and debit card payments. The new terminal provided both network (Internet) and dialup (telephone) connection paths to the bank for improved accessibility of transactions in the event Internet service was lost. Debby and Steve felt they had improved the reliability of the tools their practice depends on.

Without warning, the staff managing the front desk noticed that access to their online patient scheduling application was no longer working properly. The staff was accessing the regular website URL, but they were being taken to an incorrect website. The staff called the online provider of the software and reported the issue. The staff quickly implemented their alternate, in-house scheduling procedures.

Debby, Steve and the staff at North County Pediatrics had revised all their processes to ensure that loss of Internet connectivity or computer systems no longer had a significant impact on their ability to service their patients. Patients in the office and those calling to schedule appointments never had any idea the main Internet hosted scheduling application for the practice was offline.

Prepare and Prevent

In general, small businesses who provide their customers with IT and communications services should have system redundancy, onsite and offsite backups of system configurations and data, emergency power (UPS and generators), and automated fail-over systems in place to maintain operations with very little or no outages for services within their control. There are many interdependencies across the different critical infrastructure segments, and disruption of one of the segments may impact the others in a cascading effect; therefore, take what steps are necessary to protect your system components to minimize those impacts. IT and communications service providers should ensure compliance with applicable regulations and implement standards and procedures that align with recognized national and international standards, such as the Information Technology Infrastructure Library (ITIL), the International Standards Organization (ISO), and the National Institute of Standards and Technology (NIST). You should have a Business Operations Plan, a Security Strategy, and (to be prepared for emergencies) a Computer Security Incident Response Plan, a Business Continuity Plan (sometimes called a Continuity Of Operations Plan or COOP) and a Disaster Recovery Plan.

Non-IT savvy small businesses should have the following things provided for their business by either their IT partners or IT/communications service providers:

- Perform regular data backups, at least daily incremental changes and weekly full backup; arrange to duplicate weekly backups to keep one onsite (in a fire- proof cabinet near the server location) and send one off-site to secure storage. Off-site backups can be rotated every four to six weeks, so old data is erased and new backup data is saved, with the time period dependent on business requirements (it may actually be three or six months). Backup data should be tested regularly to ensure it can be restored without errors or data corruption.

- Implement business processes which keep client/customer data separate from other business records and from your website server. Strongly consider keeping paper copies of client records in a locked, fireproof cabinet, and ensure those are updated as necessary (such as, when new clients are added or client information changes). Ensure you are in compliance with any record keeping regulations that govern your industry/business.

- Have IT staff enable computer and network audit logging and actually read the logs for error messages and anomalies. If there is unusual activity in a log, research its cause and take necessary steps to prevent any malicious activity.

- Keep your servers and office computers up-to-date with current versions of anti-malware, and other security software, as well as keeping the operating systems patched with current security releases.

- Secure any wireless networks by changing all default/factory passwords, especially for the administrator account, and enable WPA-2/AES encryption for mobile user accounts.

- Train your users in proper use of your systems, including Cybersecurity awareness, especially around the potential cyber threats with using the Internet and e-mail on business systems. Employees should each have unique User IDs for accessing the business systems and should not share their User ID or password.

- Limit who has access to client/customer personal data to only those of your employees who need it to conduct your business.

- Implement and monitor Internet filtering to block access to unwanted and potentially malicious websites (such as pornography and gambling) that are not required for your business. Some of these sites are the main source of hidden malware.

Small businesses should have a Business Operations Plan, including emergency procedures that may involve using manual processes when normal systems and communications are not functioning. In your Business Plan, you should consider Cybersecurity (and the required tools to implement it) as an investment, similar to insurance, just not as an expense. Think about the value of your business data in relation to the amount it costs to protect it, including loss of clients and harm to your business reputation if the data is stolen or corrupted.

Respond

Consider monitoring the network traffic of the compromised system for a short time before disconnecting it or taking it offline; sometimes, it is possible to capture remote IP addresses or to detect other compromised systems. Depending on your type of business, be sure you comply with any federal or state regulatory requirements for notification of customers, and also strongly consider notifying your local law enforcement agency or the FBI, even if it's not required (your incident may have been part of a larger series of attacks, which they might be tracking).

Recover

Once you have taken the necessary steps to stop the cyber attack and keep your business running, even at a minimal level, now it is time to work on restoring business as usual to full operation. When all your computer systems have been checked and cleaned of any malware and other system problems are corrected, it's time to restore your backup data and then bring the online data current with whatever manual transactions took place during the incident. You might need to continue some manual operations concurrently, while the systems are brought back into service and updated. After all systems have been restored and brought up-to-date with current transaction data, be sure to create a fresh set of full backups (making a duplicate to send to a secure offsite storage site), and update all system configuration documentation (also keeping a copy offsite).

If you are relying only on your Internet Service Provider (ISP) to keep you safe from malware, you are doing yourself, your staff and your customers a disservice. Unless you lock the thumbdrive and CD capabilities - malware can be passed by simply inserting an infected thumbdrive or CD. Make sure you have your staff policies and procedures manual up to date at all times.

CAUTI
RADIOAC

Nuclear Reactors, Materials, and Waste

This sector includes the facilities, radioactive materials and waste related to: nuclear power plants; non-power nuclear reactors used for research, testing, and training; manufacturers of nuclear reactors or components; nuclear fuel cycle facilities; and decommissioned nuclear power reactors. While cyber threats to Nuclear power plants and nuclear waste may be more publicized, there are also a great many other uses of radiation and nuclear materials which may be vulnerable to cyber risks.

In addition to those areas related to power generation, the sector also covers radioactive materials used primarily in medical, industrial, and academic settings, as well as the transportation, storage, and disposal of nuclear and radioactive waste from any source. It is in these non-power applications where small/medium businesses are likely to be involved.

Modern medical radiation systems may be vulnerable to cyber manipulation, including x-rays for radiology, computerized tomography (CT), and nuclear medicine, as well as medical systems for delivering radioactive materials for diagnostic, medical therapy and sterilization.

Many industrial applications including sterilization of health care products and pharmaceuticals, irradiation of food and agriculture products, materials modification, and the production, storage, use and measurement of various radio-isotopes and markers can also have significant cyber and physical vulnerabilities.

Local Healthcare Product Manufacturer

An ACME Healthcare Products, Inc. cabling technician, while working in the control room of the company's gamma irradiation production control facility, incorrectly identifies several adjacent Ethernet switches while installing an Ethernet patch cable. He is then interrupted with an urgent call, and the error remains undiscovered. While one of the switches is part of the corporate communications network fabric, the other serves an isolated network providing control room access to the on-line management computer system controlling the Cobalt-60 gamma irradiator being used for sterilization of health care products, including surgical gloves.

A little later, after a patient died from a post-surgery infection in a hospital, a family member who happened to be a university computer science student, jumped to the conclusion that the ACME surgical gloves the doctor wore must be the culprit, and plotted to wreak havoc on that particular brand. He begins by visiting the ACME's website and gathered information from various message boards. Over time, he mapped out ACME's IT infrastructure, and discovered the miss-configured network connection.

Upon gaining access to the Cobalt-60 irradiator controller, he changed the software driver to indicate the correct dosage, while actually delivering one-millionth of the correct dosage every time gloves are being irradiated. Only after thousands of surgical gloves have been distributed across the country, is the lack of sterilization discovered.

The ACME company Brand is no longer trusted, significant revenue is lost, hundreds of potential medical claims are working their way through the courts, and a number of investigations are underway.

Lessons Learned:
Correct Network architecture and isolation is critically important, and must be part of the overall active monitoring program.

Never depend entirely on network isolation or security zones to protect attached devices. Always configure routers, firewalls and devices assuming they may become exposed to direct and indirect attack.

Design and implement network and control systems to be as implementation error-proof as possible. Include routine audits and monitoring to assure correct configuration. Design network connectivity to be as "dark" as possible, so when errors are made, defense in depth can provide a higher level of Confidentiality, Integrity and Availability.

Maintaining accurate documentation and labeling is critical for good cyber hygiene.

High Technology Dental Clinic

The DentalAce Clinic network supports a reception area, three operatories and orthodontic laboratory. All are interconnected with the latest in on-line scheduling, digital radiography, electronically maintained chart system and VOiP based communications system for both intra-office flagging/paging, and external Internet based voice/voicemail communications.

Recently an IP camera system was installed for both security monitoring, as well being able monitor the office activity level from inside and outside the office on various monitors and on their smartphones. Several months later they started to notice a significant sluggishness in their network. Subsequently, numerous videos surfaced on YouTube embarrassing several patients.

Upon review, it was discovered that inbound UDP port 13364 had been left open on the firewall/router, and a remote administration vulnerability had been exploited on the cameras. Subsequently a camera's Linux system was discovered to have been hacked permitting attacks on other computers in the local network.

Subsequently a machine hosting bridge software interconnecting the electronic records and radiography machines had been penetrated, and an exploit in the bridge software command line interface for the radiography machine permitted dosage levels to be manipulated remotely.

Lessons Learned:
Document and maintain accurate network mapping and machine configuration documentation.

Good practice dictates network isolation techniques are necessary, particularly with critical devices. This may dictate carefully managing information flow to only authorized devices. While full interconnection may look great, it is imperative to restrict information flow on a need-to-know basis.

Regularly check and update all operating system, application, and firmware resident in all attached devices, paying particular attention to the firewall/router, printers, cameras, IP connected medical equipment, etc.

Understanding the potential security vulnerabilities before installing new or replacement equipment.

Conduct regular penetration testing and monitor security configurations.

Prepare and Prevent

The above Cybersecurity scenario's may not rise to the level of other types of emergencies, such as natural disasters, it is still one that must be considered as more and more businesses employ technical solutions that connect to networks. If it connects to a network it is susceptible to cyber-attack so you must provide reasonable care and maintain it.

This section deals with making risk-based business decisions, what steps should be taken to prepare for the inevitable, what security measures should be put into place to help make your business be less of a target and to minimize its impact to your business.

The following general action items apply to maintaining a basic level of cyber-hygiene for your business, with the expectation there will be differences in the level of detail and the manner of implementation due to business type, compliance requirements and federal/state regulations.

- Create a basic Cybersecurity Incident Response Plan, this should include basic steps for your staff to follow. Include a contact matrix with a list of names and phone numbers so they know who to reach in case of an incident.
- Educate all staff on safe Cybersecurity practices to help prevent an incident, the latest information on such topics as social-engineering, phishing and basic cyber-hygiene practices they can follow to protect themselves at work and at home when online.
- Use strong passwords or a solution such as single sign-on to reduce the "yellow-stickies" with passwords stuck on them that seem to lay around offices. The key point here is don't make it easy but don't make it too hard that people will go around it and circumvent the security control.
- Remind your personnel that they are to only disclose personal or financial information on reputable sites and via a secure network connection.
- Regularly confirm your company's compliance with internal security policies and any regulatory standards.
- Be suspicious of any anomalous computer or network behavior and report it to your IT staff to be investigated and remediated.
- Implement at least a layered network (firewall, patching, encryption, back-ups) and end-point security (anti-virus, anti-malware) protection.
- Identify what types of information you process, where it is stored, how you manage it, what compliance regulations pertain to it and how your personnel use it in a daily basis.
- Backup your data from both local hard drives and shared network drives on a regular basis (e.g., weekly), and store an extra encrypted copy offsite.

- Restrict access to resources and information to those that actually need it, periodically audit this access and update where necessary.
- Image and/or retain hard drives from employees who leave under less than amicable circumstances or who had access to confidential data.
- Enable computer and network logging, and store logs offline.
- Treat every cyber incident as potentially malicious until it is determined otherwise.

Respond

You have discovered a potential Cybersecurity incident, now what do you do? Did you put the aforementioned Cybersecurity policies and procedures in place? Did you create your Cybersecurity Incident Response Plan – with its contact matrix? If not, then it's time to implement one!

This section covers some the steps you should take when you have a potential breach, malware or other Cybersecurity incident. Even if it starts out as unconfirmed, there are steps you can take which can prevent the spread of malware or reduce the impact of an intrusion, while in the process of confirming if an actual Cybersecurity incident is occurring or not. Once confirmed, there are additional steps to take to stop the attack, minimize or mitigate the damage to data or systems, and minimize the overall business impacts.

The following general action items apply to helping your business stay resilient as you manage this incident. Remember, there will be differences in the level of detail and the manner of implementation due to business type, compliance requirements and federal/state regulations.

- Contact authorities. Fast responses are important in cases with active data exfiltration such as customer or financial data. Having a Cybersecurity Incident Response Plan with a contact matrix will help your staff in times like this to make sure you contact the correct authorities.
- Preserve the original hard drives of compromised systems for review by authorities. If your plan calls for a vendor or 3rd party forensic team to assess the incident, leave the compromised asset on and untouched – just remove the network cable so it is not on your network.
- Provide documentation for anything that has been done to the system since the discovery of the incident. This comes in handy if a team is assessing the compromised asset, they need to know what happened with it before it was in their custody.
- Provide copies of any network diagrams or system documentation showing the environment in which the system operated.

- If you have the skill and access to the asset, identify and copy any internal or external log files (i.e. intrusion detection system or firewall logs). If not, be prepared to provide access to your vendor or 3rd party forensic team.

- If you have the skill consider monitoring the system's network connections prior to taking it offline because other compromised systems or suspect IP addresses can frequently be identified. Otherwise request your vendor or 3rd party forensic team provide this information to assist in the investigation and remediation of the incident.

Recover

The incident is over and your business may have suffered minor, moderate or major impacts. How well did you Prepare and Prevent, and then Respond to the incident?

Even with proper preparation and response, steps must still be taken to get the business back to normal operations. This final section provides certain steps to take, based on following the action items in the prior sections, to help keep the business running during the immediate aftermath of an incident and then continuing to fuller recovery. It should be noted that, even with the best preparation and response, a major Cybersecurity incident could cause catastrophic, unrecoverable damage to a small/medium business. Following the basic steps outlined above and in this booklet are intended to increase a business' chances of being able to recover and restore operations.

The following general action items apply to any business, with the expectation there will be differences in the level of detail and the manner of implementation due to business type, compliance requirements and federal/state regulations.

- Find a safe place to re-start operations – this might be the normal office space, if there was no disaster which caused physical damage; or this might be an alternate location, set up temporarily to be able to conduct business.

- If you are unable to use your computers (e.g., network services are not available), and the nature of your business allows it – conduct business manually and keep track of all transactions on paper.

- If computer equipment was damaged or is being kept as evidence, arrange to lease or buy new computer equipment, and have it installed and configured for your business use. Consider getting Cybersecurity insurance (before an incident occurs), to help pay for replacement equipment and data restoration.

- If you will be using existing computers, ensure they have been "cleaned" of any malware (reformat the hard drive and reload a clean image of the operating system, then install software applications).

- Restore your backup data to the point before the computers were infected or breached; test and validate the data before resuming operations with it; be sure to add any manual transactions into your system to get it up to date.

- After restoring your computers and business data, make a fresh backup of each system; store one copy at the business and store a second copy off-site in a secure place (i.e., in a fireproof cabinet).
- Notify your vendors, suppliers, distributors, customers, and other stakeholders when you resume online operations, even if it's from a temporary location.

While a clean form of energy, nuclear power is subject to disturbances in the earth and fraught with potential high risk from both cyber attack and mass contamination.

A laptop is stolen every 53 seconds, while 12,000 laptops disappear every week from U.S. airports alone. Of all lost laptops, 46% had confidential data and no encryption.

-Intel Corporation

Transportation Systems (Postal & Shipping)

Transportation has long been at the hub of commerce in the U.S. and plays a key role in our distributed business models, let alone helping to ensure families separated across the nation are able to safely travel.

Our structured air traffic control systems, entailing pinpoint accuracy and timing of airplanes, fosters our quality of life; while the Interstate roadways, developed after World War II to transport goods across the nation, are still foundational to the U.S. commerce system.

Disruption or loss of our transportation systems can and have had a profound impact on business. Just think of the amount of money lost when one a single airplane is cancelled due to a mechanical failure. On top of that, consider the reputational impact for the carrier and frustration of the customers.

Examples for transportation:

- "Fast Track" payment on Toll-roads
- Overnight package service
- Airline scheduling and tracking
- Airline booking
- Piggy-back services between trucking and rail services

American ports, terminals, ships, refineries, and support systems are vital components of our nation's Shipping critical infrastructure, national security, and economy. A successful cyber-attack on America's shipping infrastructure could cripple our backbone of commerce. Many smaller shipping service providers, such as a local shipping office and transportation depot may be on-ramps for attacks affecting an entire system. Compromised data anywhere in the system can have a significant ripple effect across an entire supply chain. Hacking in to a local shipping/postal company's database could yield highly sensitive customer data including cargo routing and handling data as well as credit card information. Data regarding time critical, special handling and hazardous materials are all viewed as particularly sensitive cyber targets.

On a national scale, even a minor cyber-attack could potentially cripple food distribution, facilitate the smuggling of people or import weaponry that can present a high risk to our nation.

Businesses in Acton

Transit Company

Mass Transportation & Delivery, Inc. was a transportation and transit company that monitored and controlled the movement of goods and people. One week, a "glitch" kept returning in their systems that disrupted all of their logistics and operations.

A professional realized that they had been breached and their network was compromised. Immediately they shut down all of their services to avoid any other issues. A local store in San Diego used the services of Mass Transportation & Delivery, Inc. twice a week to keep their inventory and resources stocked. When the supplier stopped service, the storeowners did not know whether they could stay open or even survive as a company with the disruption. Their inventory was depleted quickly and it looked as if they would have to close their doors. The manager of the local shop spoke to a couple employees at the adjacent store.

Apparently their company had also used Mass Transportation & Delivery, but they appeared to still be receiving deliveries. The manager knew it was time for discovery if he wanted to stay in business. He needed to seek alternative sources - hopefully it was not too late.

Business-Critical Presentation

Tom Swedmill was an entrepreneur and owned a small software company in Southern California. The opportunity of his life had just fallen into his lap. The government asked him to come and present the latest version of his new application to the SBA and military generals in Maryland. The first leg of his trip was uneventful except for the turbulence as they approached Chicago. It was a bit more than he was really comfortable with - the very reason why he typically booked only non-stop flights. The landing was a bit rough as well with large storm cells racing towards the airport. Tom reassured himself that this happened all of the time in Chicago and they were experienced in handling "issues." He exited the plane and ran to look at the departure board and verify his next gate. When he approached, he saw a large group of people looking too. The board showed his flight - CANCELED! His heart sank and he reached for his cell phone to look for options. In a split second, the entire board went blank for a second and then came back to life. However, the airline names and flight numbers no longer matched the city and gate numbers just displayed. Seconds later, each flight at the bottom of the screen started disappearing and was replaced with a URL. In areas closed off to the public, the airport's head of IT and his computer SWAT team scrambled. Millions of dollars were lost with each minute that ticked away...

We Post For You, Inc.

Pat Wilson owns a national shipping and postal store franchise. One of their largest customers (an eBay reseller) complained his credit card number had been stolen. The customer assured Pat this particular card was only used for business purposes and that 100% of its activity was at Pat's store. Pat called in a security expert and found that his anti-virus software had expired months ago and that his computers were vulnerable to attack and at extremely high risk. Upon discovery of key-logging malware, Pat had to now notify all 5,000 of his customers of this breach. Since the cyber-attack occurred, Pat has noticed a significant drop in his regular customers' visits and some of his most valued customers don't even frequent his shop. He had heard of cyber-attacks but thought only the large organizations were targets. With a significant decline in Pat's business (nearly 48%) he must consider options to recover his long standing customers and his now tarnished reputation.

CCC - Cargo Enterprises

CCC Cargo Enterprises is a local shipping company with ties to both the piggyback systems with the railroads and international cargo carriers between the U.S. and Asia. They recently lost 25% of their revenues and a multi-million dollar shipping contract – a result of cargo theft. Sandra Jones, the office administrator, had recently run into some financial challenges. Her husband lost his job, her son was sent to a juvenile detention center for selling drugs. The family life was a mess. Sandra gathered the courage to share her woes with her boss. She went into his office sharing the sad story and asked for a small raise since it had been five years since she had one. The boss's response. "Sorry, sweetie. While you do a good job we just cannot afford it now." Sandra knew better, or thought she did. Part of her job was to send the billing statements out for the office. She saw millions of dollars being billed. What she didn't see was the expense side.

That said, she told her boss the next day that she needed to stay late and catch up on all of the things he has said were urgent. He agreed. With access to systems well above her pay-grade Sandra set out to "help herself " to the funds she felt she needed and her boss wouldn't miss!

Sandra changed the company's tracking system that allowed just a small percentage of shipments to be re-routed giving her the ability to steal about .5% of the cargo without being tracked or caught. She didn't think the company would miss such a small amount. She had become part of a cargo theft ring with just a few keystrokes.

Cargo theft rings cause up as much as $30 billion in losses each year. Any product being shipped is potentially a target, but cigarettes, pharmaceuticals, and especially computer/electronic components are currently high-value favorites for being re-sold on the black market.

Prepare and Prevent

Backup plans are the best way to prepare for most challenges. Alternative information, supply and distribution plans are essential if you're primary system fails for any reason. Depending on what resources you still have, backup fuel and supplies can help you carry out some of your transportation personally. With perishable goods, make sure your delivery methods are functioning before you allocate the goods to be shipped. Consistently perform preventative maintenance on any vehicles or other transportation mechanisms. Develop your network to create relationships that could help you in a time of need.

As in all cases of cybercrime, fundamental steps are key to preparation and prevention. It is imperative to keep all software programs up-to-date, including the operating systems. From time to time, computer software is "sunset" or is no longer supported. It is especially true for businesses to ensure they tune their ear for notification of changes or sunset of computer operating systems like Microsoft's Windows XP. Standard practices such as requiring complex pass-phrases, no reuse of the same pass-phrase within a year and a frequent change pattern are all-important. Staff should be trained in the basics of Cybersecurity leading practices and watch for improper behavior of their computers to report to IT professionals, whether they are internal staff or a service. Write your disaster plan – whether it is cyber or physical – you will want to have your plan in hand and know what you need to do long before you must act.

An annual risk assessment is recommended. Begin by assessing what parts of your business are controlled or supported by computer systems. Then determine what the consequences would be should those systems become inoperable, controlled by outside parties, or misused by internal parties. This should include identifying and adoption of appropriate security and management practices.

Consider your supply chain and the cyber/data vulnerabilities and practices of your suppliers, customers and other organizations critical to your company's profitability. Discuss cyber security with those organizations and incorporate good cyber-hygiene. Restrict and carefully manage access both at the cyber level and physical of your organization.

Respond

Assessment of all aspects and details is mandatory. Assumption should not be part of the equation – only facts without emotion. The transportation response will likely be creative and suited to the particular situation based upon business or personal need. The primary response is to draw on what resources and connections you already have while seeking and building a network. Protect travel sources you have access to and seek alternative methods. Community circles play a large role in how businesses can function in the case of a disaster aftermath.

Small businesses also come to the forefront in many cases because of their tight network and local ties. A can-do, make-do attitude and creative approach to solving problems will allow business to survive or even flourish. As the saying goes: "necessity is the mother of invention."

How you respond in a time of disaster – cyber or physical – can make the difference of your ability to recover fully, somewhat or not at all. Some key things to consider when disaster strikes are: if you see something – say something! Report suspicious things to the proper authorities. Alert the authorities if you suspect your organization has been breached or compromised. Change your pass-phrases immediately. First change your pass-phrases for each account especially for financial or mission critical systems and do not reuse the same pass-phrase in the future. If you suspect malicious code, disconnect your computers from the Internet and consider restarting them in "safe mode" and do a full restore systems. Also, be sure to inform your partners, affected customers and supply chain including banks or credit card companies. This is where building your plan before an incident arises helps you to keep a cool head. You may wish to consider closing any accounts that may have been compromised and watch for any unexplained or unauthorized charges or shipments on your accounts.

Recover

The aftermath of a disaster, whether it is physical or cyber, can be beneficial to a business if they have planned well and use the situation to analyze business priorities, resources and advantages. Build your customer base through referrals and streamline operations through alternative sources and perhaps even new contracts. Re-establish your prior delivery methods if possible, and coordinate with others to maximize efficiencies – especially in the local community.

Now is the time to implement your plan. You will want to file a formal report with the local police so there is an official record of the incident. You should also submit a report to the FBI if your organization is involved in inter-state commerce or the crime touches multiple states, the United States Secret Service (USSS) Electronic Crimes Task Force and/or the Internet Crime Complaint Center. You should also consider what information that may have been compromised, and contact all appropriate agencies. Most of all, stick to your plan and focus on rebuilding your organization. Share with your partners, customers and others. Help the community by sharing your story so that you may help others learn from your experience.

Water and Wastewater Systems

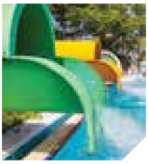
There are approximately 160,000 public drinking water systems and more than 16,000 publicly owned wastewater treatment systems in the United States. Approximately 84 percent of the U.S. population receives their potable water from these drinking water systems, and more than 75 percent of the U.S. population has its sanitary sewerage treated by these wastewater systems.

Many drinking water and wastewater utilities today depend on computer networks and automated control systems to operate and monitor processes such as treatment, testing and movement of water.

These industrial control systems (ICSs) have improved drinking water and wastewater services and increased their reliability. However, this reliance on ICSs, such as Supervisory Control and Data Acquisition (SCADA) systems, has left the Water Sector and other interdependent critical infrastructures, including energy, transportation, and food and agriculture, potentially vulnerable to targeted cyber-attacks or accidental cyber events. A cyber-attack causing an interruption to drinking water and wastewater services could erode public confidence, or worse, produce significant public health and economic consequences.

Just Juice It

Just Juice It is a San Diego juice bar that specializes in fruit smoothies and specialty health drinks. In order to make the drinks the juice bar relies heavily on their local water utility to provide their ice and water. Early Saturday morning, Jimmy decided he wanted a fruit smoothie to start his morning off right. As he was walking to the Just Juice It location he noticed a huge line outside. He thought since Just Juice It was a new popular place this was normal for a Saturday morning. In reality the juice bar wasn't getting water from the local water utility limiting their ability to quickly make drinks and smoothies due to the lack of water and ice. Luckily as part of their emergency preparedness plan the juice bar owners had planned for this scenario and kept enough emergency ice and water to maintain operations for up to four hours. Even though service may have slowed Just Juice It still had the ability to make drinks and money thus making Jimmy's Saturday morning.



Wally's Water World

Southern California is a great area to own and operate a large water amusement park. Wally Valdez, a San Diego water park owner, relies heavily on the park's water treatment and distribution system to ensure proper conservation and operation of his amusement park. As part of the semiannual maintenance checkup on the industrial control system that operates the park, the manufacturer of the system sent over a technician to perform their necessary duties to ensure the park stayed online and efficient throughout the busy summer season. All was well until about one week later when during a busy Saturday afternoon the park's entire water system shut down. Rides weren't pumping water, recycling and treatment of water stopped, and customers were forced to leave the park. Wally's Water World incident response plan was immediately put into action.

After all the customers calmly and safely left the park, Wally went scrambling to figure out who did what and when. The interesting thing was no one had touched the water industrial control system in days. In fact the last person to touch anything was the technician from the system manufacturer. The park was shut down for several days as forensics investigators from local law enforcement investigated the situation. It was determined the technician's workstation was infected with malware, and once the technician plugged his computer into the waterpark's system, the malware infected the industrial control system thus causing the failure. Wally learned to make sure to ensure anyone touching his computing infrastructure was doing so with approved and clean equipment.

Prepare and Prevent

Water & Wastewater utilities can reduce vulnerabilities from cyber attacks or events by: (1) identifying systems that need to be protected, (2) separating systems into functional groups, (3) implementing layered or tiered defenses around each system, and (4) controlling access into, and between, each group. Utilities should also:

- Institute procedures to limit number of individuals with authorized access to networks
- Update software on a regular basis
- Require strong passwords
- Install and maintain anti-virus software
- Employ intrusion detection systems and firewalls
- To be most effective, water utility cyber security programs should build on strong organizational security policies, utility-wide security awareness
- Ensure effective personnel and physical security practices

Businesses relying heavily on water utility services should establish proper emergency preparedness supplies (such as bottled drinking water) and establish an incident response plan. Businesses should test their plans at least once a year and identify potential areas of improvement or gaps.

Respond

In case of an incident (physical, cyber, or natural) the following courses of action are recommended:

- Initiate your incident response plan
- Gain access and prepare your emergency supplies
- If you believe the compromise was caused by malicious code, disconnect your computer from the Internet
- File a report with the local police so there is an official record of the incident
- Report online crime or fraud to your local United States Secret Service (USSS) Electronic Crimes Task Force or the Internet Crime Complaint Center

Recover

Once the incident has ended, the following courses of action are recommended:

- Execute your business recovery/continuity plan
- Bring up systems in the order of priority
- Restore backups as necessary
- Hold after-action meetings. Determine lessons learned and develop improvement plans to make appropriate policy/procedure adjustments

Often, in addition to power, water is a key element of our critical infrastructure that is most often taken for granted. In most places across the United States there is an abundance. But, in the past few years, the western region of our country has experienced a severe drought. Not only has water become scarce, but both businesses and individuals are beginning to realize that we cannot take pure, drinking water for granted, when all water is in high demand. We don't even like to consider a cyber attack on our water filtration systems. We cannot exist without this precious commodity.

Cybersecurity Checklist – Business Action Items

This section provides a thorough (although not all-inclusive or exhaustive) checklist of action items within the three categories for Incident Management (Planning, Preparation, and Prevention - Response - Recovery). You should take the items that apply to your industry sector and particular business situation, and incorporate them into your Incident Response Plan, adding any other specific actions that should be taken by your business or industry that may not be listed here. If you don't yet have an Incident Response Plan, Securing Our eCITY® will be offering free templates for SMBs and others to use and customize to your business. Also, refer to the list of resources in the next section for information about Incident Management planning, response, and recovery standards and procedures.

Planning, Preparation, and Prevention Actions

□ Identify and track all critical business systems and processes which may be susceptible to compromise, including accounting, human resources, material handling, production, packaging, inventory, transportation, warehousing, scheduling, customer service/support, etc.

□ Maintain an accessible hardcopy list of applicable contacts and alternates for key customers, partners, shipping and related services, including alternate methods of communication

□ Create a Business Operations Plan, to include:

- □ Standard business procedures for normal operations, including how to maintain and secure digital business information, and how any automated business processes should function
- □ Alternate business procedures for atypical operations, including the use of paper-based or other non-automated processes and how to ensure necessary security of confidential or sensitive information
- □ Establish criteria for selecting IT Service Providers – find those which follow international or national standards (e.g., ITIL, ISO/IEC, NIST)
- □ Develop a Security Plan for manual, physical security measures to replace automated ones
- □ Ensure compliance knowledge for Sarbanes-Oxley (SOX), HIPAA, FISMA and other applicable laws or regulations

□ Develop a Disaster Recovery Plan & Business Continuity Plan (also called a Continuity of Operations Plan or COOP), together referred to as a "DR/BC Plan," taking into account the following:

- □ Coordinate emergency plans with suppliers & primary customers
- □ Plan for manual or alternative business operations
- □ Plan for local emergency power generation, if necessary
- □ Plan for emergency fuel supplies (onsite storage or delivered)
- □ Use Uninterruptible Power Supply (UPS) with battery back-up for all IT equipment

- □ Plan for how to conduct offline financial transactions (e.g., cash); coordinate a plan in advance with your financial institution
- □ Develop written procedures for system shutdown, lock-out, and re-start
- □ Plan for retrieving and restoring backup data
- □ Plan for moving business operations to an alternate facility/site

□ Educate staff on Business Operations Plan, DR/BC Plan, as well as policies and procedures related to protection of company assets (including data) and general cyber security practices

- □ Conduct quarterly, bi-annual or as needed
- □ Perform an assessment of the training – did they "get" it
- □ Use practice situations, drills, exercises, etc. as a type of training

□ Develop acceptable use cyber policies including:

- □ Internet access, Blacklisted websites, Social media, etc.
- □ Define permissible online activities, as well as prohibited ones
- □ Ensure employees are trained on the policy and sign an acknowledgement (possibly annually)

□ Implement Cybersecurity Best Practices:

- □ Backup business data (daily – incremental / weekly - full) onto encrypted media and store copies offsite
- □ Keep all systems updated with anti-virus and anti-malware security software, including automated patches and updates
- □ Keep all computer operating systems updated with current security patches
- □ Secure wireless networks with strong passwords (remove factory defaults); hide the broadcast identifier (SSID) to reduce "drive by" attacks
- □ Have IT staff enable and monitor system and network audit logging
- □ Ensure compliance with all relevant regulatory requirements (e.g., FISMA/FIPS)

- □ Limit who has direct access to client records to only those who need it
- □ Implement Internet traffic monitoring and filtering (block unwanted sites)
- □ Train employees in Cybersecurity and proper use of business systems
- □ Keep customer/client data stored separately from any public access website
- □ Keep a paper backup copy of client records (safely and securely stored)

□ Develop a Computer Security Incident Response Plan

- □ Maintain inventory of computer assets (hardware and software)
- □ Maintain list of IT service providers and emergency contact information
- □ Create checklist of specific actions in an event of a cyber incident (often in the form of a decision tree, so that particular actions are dependent on the nature and extent of a potential incident)
- □ Define and establish priority notification of employees
- □ Define and establish priority notification of customers/clients, as deemed necessary and at the appropriate time
- □ Define other notifications (e.g., law enforcement)
- □ Account for Regulatory Compliance (as required)

□ Conduct refresher training on emergency procedures (at least annually)

□ Have a manual (non-electric) safe or locking fireproof cabinet for secure storage of paper or other non-digital materials

□ Incorporate alternative energy sources when feasible (e.g., active solar, gas/diesel/propane powered generators)

□ Plan for conducting manual financial transaction; have emergency cash in a secure place

□ Plan for potential barter system to obtain food and other essentials (for long-term disaster situations

□ Know where to go to obtain cash

□ Plan for alternative modes of transportation

□ Plan and pre-arrange alternative ordering methods with current suppliers

□ Plan alternative for food preservation, preparation, and distribution

- □ Plan alternative methods for obtaining fuel and supplies
- □ Coordinate alternative delivery plans with suppliers and customers to minimize losses
- □ Plan to ensure security of emergency cash and credit/debit cards
- □ Plan how to protect valuables

Response Actions

- □ Identify impacted/compromised systems and assess damage
- □ Implement cyber incident response plan actions (emergency/contingency plans) to minimize losses
- □ Attempt to preserve evidence while disconnecting/segregating affected systems
- □ Obtain system configuration, network, and intrusion detection logs. Note any configuration changes (before and after incident). Preserve hard drive(s) from compromised system, if possible
- □ Notify appropriate authorities and request assistance, if necessary
- □ Reduce damage by removing (disconnecting) affected computers
- □ Implement manual tracking and controls
- □ Coordinate with suppliers and customers for long-term needs
- □ Implement alternate delivery methods with suppliers & customers
- □ Plan for alternative modes of transportation
- □ Know where to go & how to implement cash or barter transactions for transportation
- □ Minimize travel until services are restored
- □ Ensure security of emergency cash and credit/debit cards
- □ Protect valuables (the company's and also employees' or customers')
- □ Coordinate with others in the immediate area and (if possible) peer businesses; share information & resources, as appropriate

Recovery Actions

□ Make "checkpoints" (also called "recovery points") frequently, and take actions to restore systems to normal configurations

  □ Use backup data to restore systems to last known "clean" status

□ Store backups in a physically and environmentally secured location (onsite or offsite, or both)

□ Update restored systems with current data (from manual transactions)

□ Create new "clean" backup after data has been updated

□ Continue manual or alternate operations processes/procedures until emergency, disaster or cyber incident is declared over and business is allowed to return to normal operations

□ Re-establish ordering and shipping processes, as necessary & available

□ Coordinate with others (suppliers, partners, distributors, & customers); share information & resources, as appropriate

□ Re-establish business operations when feasible; bring up critical systems & operations first

Additional Resources

Securing Our eCITY® Foundation
http://securingourecity.org/
http://securingourecity.org/resource

U.S. Department of Homeland Security, National Cyber Security Division, U.S. Computer Emergency Readiness Team (US-CERT)
https://www.us-cert.gov/

Department of Homeland Security's Stop. Think. Connect.™ campaign - receive a monthly newsletter with Cybersecurity current events and tips
https://public.govdelivery.com/accounts/USDHS/subscriber/new?topic_id=USDHS_136

CERT Coordination Center (CERT/CC), Carnegie Mellon University, Cyber Security Incident Management (guidelines and procedures)
http://www.cert.org/incident-management/

For further information on preventing and identifying threats, visit US-CERT's Alerts and Tips pages
https://www.us-cert.gov/ncas OR http://www.ready.gov/cyber-attack

National Institute of Standards & Technology (NIST), Computer Security Resource Center (national Cybersecurity standards)
http://csrc.nist.gov/

NIST SP-800-144 – "Guidelines on Security and Privacy in Public Cloud Computing" (80-page PDF document)
http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf

San Diego Gas & Electric [offers both businesses and families tips on what to do if there is a black out]
http://www.sdge.com/safety/emergency-preparedness/emergency- preparedness

Identity Theft Resource Center (ITRC)
http://www.idtheftcenter.org OR call 1-888-400-5530

San Diego Internet Crimes Against Children (Multi-Agency Task Force)
http://sdicac.org

San Diego Chapter – ISACA
http://isaca-sd.org/

San Diego Computer And Technology Crime High-tech (CATCH) Response Team
http://www.catchteam.org/

SANS Institute, Information Security Resources
http://www.sans.org/security-resources/

Internet Crime Complaint Center (IC3)
http://www.ic3.gov/default.aspx

Information Systems Security Association (ISSA)
https://www.issa.org/

Cloud Security Alliance Guidance
https://cloudsecurityalliance.org/

Systems Security Engineering - Capability Maturity Model (search for "21827" and accept download agreement)
http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

Common Criteria for Information Technology Security Evaluation
http://www.commoncriteriaportal.org/

The Center for Education and Research in Information Assurance and Security - Purdue University
http://www.cerias.purdue.edu/

National Security Agency - Information Assurance
https://www.nsa.gov/ia/index.shtml

San Diego Supercomputer Center
http://security.sdsc.edu/

Information Resource Support Environment (Defense Information Systems Agency) - Security Technical Implementation Guides
http://iase.disa.mil/Pages/index.aspx

Cyber Security & Information Systems - Information Analysis Center
https://www.csiac.org/

California Civil Code §1798.29 & §1798.82 (aka "SB-24") – Breach Notification Law
http://leginfo.ca.gov/pub/11-12/bill/sen/sb_0001-0050/sb_24_bill_20110831_chaptered.html

Notes

Bringing IT Home –

Critical Infrastructure for Small Businesses: Prepare, Prevent, Respond, & Recover

4th Edition, Fall 2015

This book is provided as a free resource to businesses that want to learn how to protect themselves against some of the common Cybersecurity threats to the critical infrastructure sectors. The information provided in this book should be considered as basic recommendations to help with an immediate Cybersecurity incident, and as a starting point to develop a Cybersecurity plan customized to the business. It is not intended to be either all inclusive of the security measures and procedures a business should implement, nor as a substitute for getting professional Cybersecurity assistance.

Securing Our eCity® Foundation's Vision: To create a safe digital neighborhood that is both resistant to cyber-threats and resilient to man-made or natural disasters, where our citizens, businesses, organizations and government can effectively and securely navigate, collaborate, and conduct business to remain economically competitive in today's fast-changing technological environment.

Securing Our eCITY
Foundation

Securing Our eCity® Foundation
610 West Ash Street, Suite 701
San Diego, California 92101
www.securingourecity.org

This book has been sponsored by ESET® North America and San Diego Gas & Electric