Region 5
Cyber Dawn
Tabletop Exercise (TTX)

Situation Manual
October 30, 2018

This Situation Manual (SitMan) provides exercise participants with all the necessary tools for their roles in the exercise. Some exercise material is intended for the exclusive use of exercise planners, facilitators, and evaluators, but players may view other materials that are necessary to their performance. Use of the SitMan by all exercise participants is unrestricted.

THIS PAGE LEFT INTENTIONALLY BLANK

CONTENTS

GENERAL INFORMATION

Participant Roles and Responsibilities

The term participant encompasses many groups of people, not just those playing in the exercise. Groups of participants involved in the exercise, and their respective roles and responsibilities, are as follows:

Players. Players are personnel who have an active role in discussing or performing their regular roles and responsibilities during the exercise. Players discuss or initiate actions in response to the simulated emergency.

Observers. Observers do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise.

Facilitators. Facilitators provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key Exercise Planning Team members may also assist with facilitation as subject matter experts (SMEs) during the exercise.

Evaluators. Evaluators are assigned to observe and document certain objectives during the exercise. Their primary role is to document player discussions, including how and if those discussions conform to plans, policies, and procedures.

Exercise Structure

This exercise will be a multimedia, facilitated exercise. Players will participate in the following modules:

- Phase 1: Preparation
- Phase 2: Detection
- Phase 3: Escalation
- Phase 4: Notification
- Phase 5: Containment, Eradication, and Recovery

Each module will begin with a multimedia update that summarizes key events occurring within that time period. After the updates, participants will review the situation and engage in a moderated plenary discussion.

Exercise Guidelines

- This exercise will be held in an open, low-stress, no-fault environment. Varying viewpoints, even disagreements, are expected.
- Respond to the scenario using your knowledge of current plans and capabilities (i.e., you may use only existing assets) and insights derived from your training.
- Decisions are not precedent setting and may not reflect your organization's final position on a given issue. This exercise is an opportunity to discuss and present multiple options and possible solutions.
- Assume cooperation and support from other responders and agencies.
- Problem-solving efforts should be the focus of the exercise. Issue identification is not as valuable as suggestions and recommended actions that could improve prevention, protection, mitigation, response, and recovery efforts.
- Situation updates, written materials, and resources provided will be the basis for discussion; there will be no situational or surprise injects.

Exercise Assumptions and Artificialities

In any exercise, assumptions and artificialities may be necessary to complete play in the time allotted and/or account for logistical limitations. Exercise participants should accept that assumptions and artificialities are inherent in any exercise, and should not allow these considerations to negatively impact their participation. During this exercise, the following guidelines will apply:

- The exercise is conducted in a no-fault learning environment wherein capabilities, plans, systems, and processes will be evaluated.
- There is no "hidden agenda" nor are there any trick questions.
- The exercise scenario is plausible, and events occur as they are presented.
- All players receive information at the same time.
- The scenario is not derived from current intelligence.

Exercise Evaluation

Evaluation of the exercise is based on the exercise objectives and aligned core capabilities. Players will be asked to complete participant feedback forms. These documents, coupled with facilitator observations and notes, will be used to evaluate the exercise and compile the After-Action Report (AAR).

SECTION 2: EXERCISE SUMMARY AND SCENARIO

RESPONSE PLAN VALIDATION

Exercise Name	Cyber Dawn
Exercise Date(s), Time, and Location	October 30, 2018 11:00 pm – 3:30 pm Pierce County Emergency Management Policy Room 2501 South 35th Street, Suite D, Tacoma WA 98409
Scope	This exercise is a facilitated, discussion-based exercise, with a planned duration of four hours. The exercise will build the foundation of local cyber incident management.
Mission Area(s)	Response
Core Capabilities	Planning, Cybersecurity, Intelligence and Information Sharing, Operational Coordination, Situational Assessment, Public Information and Warning
Objectives	1. Increase cybersecurity awareness to senior officials of cyber risk management, cyber related planning, and other issues related to cyber incident prevention, protection, response, and recovery of critical systems. 2. Assess cybersecurity integration into an organization's all-hazards preparedness. 3. Examine cybersecurity incident information sharing, escalation criteria, and related courses of action. 4. Examine cybersecurity incident management structures. 5. Review cyber resource request and management processes.
Threat or Hazard	Cyber
Scenario	A hacker exploits a software vulnerability and conducts spearphishing to steal personally identifiable information and protected health information from government systems. Additionally, malware capable of opening cell doors at a local prison is discovered.
Sponsor	Pierce County Emergency Management (PCEM) State Homeland Security Program (SHSP) Grant Department of Homeland Security (DHS) – National Cyber Exercise and Planning Program (NCEPP)

Participating Organizations	Twenty-five-plus participants from state, local, public, private, critical infrastructure, and tribal agencies.
Points of Contact	Natalie Stice Homeland Security Coordinator Pierce County Emergency Management 2501 South 35th Street, Suite D Tacoma, WA 98409 253-798-3311 natalie.stice@piercecountywa.gov DHS National Cyber Exercise and Planning Program (NCEPP) (703) 235-5641 cep@hq.dhs.gov
Additional Information	Additional Information This exercise was designed for an organization to validate its newly drafted cybersecurity incident response plan and improve its current Emergency Operations Plan or Cyber Incident Annex. The scenario focuses specifically on incident response. The scenario includes one element—spearphishing emails disguised as HR messages—that impacts all organizational departments, as well as other elements that target individual departments. Participants discuss questions after each scenario update, rather than grouped modules or phases. This format is intended to allow a step-by-step examination of current plans at a detailed level. The intended audience for this exercise includes, but is not limited to, IT staff, emergency management staff, planners, and members of the cyber incident response team.

Scenario and Questions

PHASE1 - Day 1: Gone Phishing

11:00 a.m. ─ A City of Sumner Public Works employee reports to the information technology department (IT) that he received an email from Finance directing all employees to update their timesheets in the Employee Timesheet System (ETS). The employee clicked a link in the email that opened what looked like ETS. However, after entering the user credentials, the employee received an unfamiliar error page.

Incident Questions

1. Do employees know what constitutes suspicious cybersecurity activities or incidents?
    a) Do they know what actions to take when one arises?
    b) What established processes exist for employees to report cybersecurity incidents?
2. Would any additional reports or notifications be made? If so, are designated points of contact identified?
3. What incident severity level or tier is a suspicious email?

Additional Questions

1. What training do you provide in support of your cybersecurity incident response plan, business continuity plan, disaster recovery plan, emergency operations plan cyber incident annex, or other related plans?
2. Does your organization provide basic cybersecurity and/or IT security awareness training to all IT users (including managers and senior executives)?
    a) How often is training provided?
    b) Does it cover:
        i. General jurisdiction, department, and/or agency policy review,
        ii. Roles and responsibilities,
        iii. Password procedures, and
        iv. Whom to contact and how to report suspected or suspicious activities?
    c) What security-related training does your organization provide to, or contractually require of:
        i. IT managers
        ii. system and network administrators
        iii. vendors
        iv. other IT personnel having access to system-level software

2. Discuss your organization's intrusion detection capabilities and analytics that alert you to a cyber incident.

PHASE 2 - Day 1: Gone Phishing (cont.)

3:00 p.m. ─ The City of Sumner Service Desk receives five reports of emails similar to the one reported by the Public Works employee. Further investigation reveals that spearphishing emails were sent to employees across all Sumer departments over a two-day period. The emails directed users to a spoofed website designed to capture ETS user credentials.

Incident Questions

1. What is the incident severity level or tier of this incident once multiple spoofed emails are reported? What would prompt a change in tiers?
2. What immediate remediation and protective actions would be taken at your agency?
    a. Who is responsible for those actions?
    b. Have these options been documented in plans?
    c. How are they activated?
3. Would any additional reports or notifications be made? If so, are the primary, secondary, and tertiary points of contact identified?
4. What are the requirements and/or processes to notify agency leadership of a cyber incident at each severity tier?
5. Are these criteria the same across the enterprise, or do they differ by agency?
6. What resources and capabilities are available to analyze the intrusions:
    a) Internally?
    b) Externally though government partners?
    c) Through the private sector?

Additional Questions

1. Discuss the role of cybersecurity in contracts with third-party support vendors and crucial suppliers. Have you discussed these types of concerns and risks with them?
2. What mechanisms and products are used to share cyber threat information within your organization and external to your organization (e.g., distribution lists, information sharing portals)?

PHASE 3 - Day 3: Zombie Attack

10:00 a.m. ─ Pierce County Road Operations WebEOC - Active Response Board updates with a new incident for a five-car motor vehicle accident on Canyon Rd & 112th St E.

10:04 a.m. ─ WebEOC shows a posting for a wildfire near Canyon Rd & 112th St E.

10:10 a.m. ─ EOC staff confirm the motor vehicle accidents and wildfire postings are fake.

1:00 p.m. ─ WebEOC updates with a new posting for a "zombie attack" on Pacific Ave S & 152nd St E. EOC personnel work quickly to have erroneous postings pulled.

Incident Questions

1. What immediate remediation actions would be taken? Who is responsible for those actions?
2. Are redundant systems in place if the impacted system(s) is compromised?
3. What is the incident severity tier of this event?
4. Do you have defined cybersecurity incident escalation criteria, notifications, activations, and/or courses of action?
    a) If so, what actions would be taken at this point? By who?
    b) Who would this incident be reported to?
    c) Would any additional reports or notifications be made (e.g., to law enforcement for reasons related to public safety)? Are points of contact identified?
    d) Would leadership be notified?
    e) Does the organization report cybersecurity incidents to outside organizations? If so, to whom?
    f) What, if any, mandatory reporting requirements do you have?
5. Are these criteria the same across the enterprise, or do they differ by agency?

Additional Questions

1. How is information shared among your internal and external stakeholders—through formal or informal relationships? What information sharing mechanisms are in place?
2. Do you have processes to ensure that your external dependencies (contractors, power, water, etc.) are integrated into your security and continuity planning and programs?

PHASE 4 - Day 4: Message Received

12:00 p.m. ─ Multiple information sharing partners contact the South Sound Regional Intelligence Group (SSRIG) regarding a hacker advertising City of Puyallup cyber vulnerabilities, inciting their exploit, and selling Puyallup tax records. The reports show that at 2:30 a.m. on Day 2, user "B1gM0n3y" posted a message in a known hacker forum alerting readers that the Puyallup government has Windows XP vulnerabilities that can be easily exploited. The user boasted that he accessed tax records from the Finance Department and is selling citizens' personally identifiable information. To prove these claims, "B1gM0n3y" posted a screenshot of the tax data.

Incident Questions

1. From which information sharing partners would you expect to receive this information (e.g., FBI, USSS, MS-ISAC, U.S. Computer Emergency Readiness Team [US-CERT])?
2. Which department/organization would receive the information?
3. How and to whom would the department/organization further disseminate this information?
4. Are there flowcharts showing the high-level relationships and crisis lines of communication (i.e., who calls who) specifically for a cyber incident? Are they part of the response or continuity planning documents?
5. What are your essential elements of information and key information questions necessary for operational and executive-level responses to cyber incidents? Where are they documented?
6. What immediate protection and mitigation actions would be taken? Who is responsible for those actions?
7. What, if any, mandatory reporting requirements do you have? Are additional reporting requirements in place for the loss of personally identifiable information (PII)?
8. At what point in the scenario would you contact law enforcement and/or the state Attorney General?
    a. How would relationships with law enforcement and other partners be managed? Where is the process documented?
    b. How does a law enforcement investigation impact containment, eradication, and recovery efforts?
    c. Are processes and resources in place for evidence preservation and collection?
    d. What are your expectations of state and federal government?

Additional Questions

1. Compare and contrast incident management when incident detection occurs internally and when incident detection originates from external stakeholders notifying your organization.
2. What cyber related public information planning has occurred?
    a. Who is responsible for public information related to the incident?
    b. Have public information officers and other spokespersons been trained on cyber specific terminology or otherwise been prepared for a cyber incident?

PHASE 5 - Day 5: On the Defensive

9:00 a.m. — After being alerted that hackers are targeting government agencies, the Tacoma-Pierce County Health Department (TPCHD) reviews its logs and finds a large amount of data has been exfiltrated from the TPCHD systems in the previous 48 hours. Bates Technical College performs a similar review and finds a similar data breach. The Pierce County Sheriff's Department (PCSD) reviews its logs and finds a rogue device on the network. Other agencies have not found evidence of any breaches at this time.

8:00 p.m. — PCSD officials recovered the rogue device—an unauthorized laptop—and discovered Supervisory Control and Data Acquisition (SCADA) malware files stored on the computer. The initial analysis of the malware indicates the malware allows for control of jail cell doors.

Incident Questions

1. Who would these incidents be reported to?
2. What, if any, additional notifications or actions would this prompt?
    a. Are points of contact identified?
    b. Are additional reporting requirements in place for the loss of protected health information (PHI)?
3. Collectively, would these events be considered the highest level of incident severity?
4. What immediate protection and mitigation actions would be taken at your agency?
5. What would the incident management structure look like? Who is assigned to key positions?
6. What resources and capabilities are required to respond to the incidents?
    a. Are these available within Pierce County?
    b. Are processes in place to request external resources or capabilities if needed?
7. Would these events trigger activation of the Region 5 Cyber Resiliency Concept of Operations? If so, would that alter any department roles and responsibilities?

Additional Questions

1. Would these events and the events of the previous five days be jointly managed?
2. Who declares the incident is over? What are the criteria for declaring the response complete?
3. Describe your role in post-incident activity.
4. What is your role in restoring and/or maintaining public confidence?
5. Have your information security officers and emergency managers jointly planned for cybersecurity incidents?
6. Are IT and business continuity functions coordinated with physical security? Are all three then collaborating with public relations, human resources, and legal departments

SECTION 3: EXERCISE APPENDICES

APPENDIX A: EXERCISE SCHEDULE

October 30, 2018	
Time	**Activity**
10:45 a.m.	Sign In
11:00 a.m.	Welcome and Opening Remarks
11:15 a.m.	Cyber Threat Landscape Briefing
11:30 p.m.	Phase One – Preparation
12:15 p.m.	Phase Two – Detection
1:00 p.m.	Phase Three – Escalation
1:45 p.m.	Phase Four – Notification
2:30 p.m.	Phase Five – Containment, Eradication, and Recovery
3:15 p.m.	EndEx, Closing Comments
3:30 p.m.	Cleanup, Closeout

APPENDIX B: EXERCISE PARTICIPANTS

Participating Organizations
Pierce County
Bates Technical College
Cascade Water Alliance
City of Puyallup
City of Sumner
City of Tacoma
Cybersecurity and Information Assurance Solutions
Franklin Pierce Schools
Pierce County Emergency Management
Pierce County Information Technology
Pierce County Sheriff's Department
Pierce County Planning & Public Works
Pierce Transit
Port of Tacoma
Puyallup Tribe
SouthSound 911
Tacoma Public Utilities
Tacoma-Pierce County Health Department
Washington State Emergency Management Division
Washington Technologies Solutions (WaTech)

SECTION 4: INFORMATIONAL APPENDICES

The following section includes background and example information related to cybersecurity threats and attacks, as well as relevant doctrine.

APPENDIX C: BACKGROUND INFORMATION

CryptoLocker

CryptoLocker is a type of malware that surfaced in 2013 and is associated with an increasing number of Ransomware infections. It restricts access to infected computers and demands the victim provide a payment to the attackers in order to decrypt and recover their files. The malware has the ability to find and encrypt files located within shared network drives, USB drives, external hard drives, network file shares, and even some cloud storage drives. If one computer on a network becomes infected, mapped network drives could also become infected. CryptoLocker appears to spread through fake emails designed to mimic the look of legitimate businesses. More information can be found at https://www.us-cert.gov/ncas/alerts/TA13-309A.

Gamer Tag Discovery

In December 2012, a network administrator of a well-known hacktivist group was convicted of conspiracy to launch denial of service attacks against multiple firms. An analysis of IRC logs and open source intelligence helped law enforcement officials identify the network administrator based on a nickname he routinely used. More information can be found at: http://www.theregister.co.uk/2012/12/14/uk_anon_investigation/.

High Orbit Ion Cannon (HOIC)

The HOIC is a popular distributed denial of service (DDoS) attack software used and made popular by a well-known hacktivist group. The HOIC overloads a server with fake visitors—a simulated flood of malicious traffic that pushes a site to its breaking point. Once a website is down, this software keeps it down. More information can be found at: http://www.gizmodo.co.uk/2012/02/what-is-hoic/.

Multifunction Printer Vulnerabilities

Recent research highlights the potential vulnerabilities of multifunction printers (MFPs). MFPs can be exploited to serve as a point of entry into a network in much the same way that workstations or servers are targeted. Research has shown that exploits can be accomplished remotely through social engineering and malware. More information on MFP vulnerabilities can be found at: http://msisac.cisecurity.org/resources/reports/documents/A-0012-NCCIC-130020120223MFPVulnerability.pdf.

Port Scan

A port scan is a method used by hackers to determine what ports are open or in use on a system or network. Using various tools, a hacker can connect to a series of ports to determine which ports are open. A hacker can then use this information to target an attack on the ports that are open, and try to exploit any vulnerability to gain access to the system. More information on port scanning can be found at: http://netsecurity.about.com/library/glossary/bldef-portscan.htm and http://www.linuxjournal.com/article/4234?page=0,0.

SQL Injection

SQL injection is a prevalent and potentially destructive attack that the Open Web Application Security Project lists as the number one threat to web applications. The attack involves the alteration of SQL statements that are used within a web application. SQL injection can be used to

perform a number of different attacks, including authentication bypass, information disclosure, compromised data integrity, compromised availability of data, and remote command execution. More on SQL injection can be found at: http://www.cisco.com/web/about/security/intelligence/sql_injection.html.

Exploitation of Business Applications

A business application or (business software) is any set of computer programs or software used to perform various business functions by business users.

Business applications are used to perform business functions correctly, increase production, and quantify productivity.

Security researchers have discovered indicators of exploitation against organizations worldwide affected by vulnerabilities related to outdated or misconfigured business applications.

Source: https://www.us-cert.gov/ncas/alerts/TA16-132A

Spear Phishing

A spear phish attack is a virtual trap set by cyber thieves that uses official-looking notifications to lure victims to counterfeit websites as a hoax.

Instead of casting out thousands of notifications randomly, hoping a few victims will bite, spear phishers target select groups with something in common. For example, the victims may work at the same company, bank at the same financial institution, attend the same college, or order merchandise from the same website. The notifications are ostensibly sent from organizations or individuals that potential victims would normally receive messages, alerts, texts, or emails from, making them even more deceptive.

First, criminals need some inside information on their targets to convince them the notifications are legitimate. They often obtain information by hacking into an organization's computer network or sometimes by combing through other websites, blogs, and social networking sites. Then, the criminals send messages containing links that appear to be authentic to targeted victims, offering various explanations to legitimize their need for personal data. Finally, the victims are asked to click on a link inside the message that takes them to a deceptive website, where victims are asked to provide passwords, account numbers, user IDs, access codes, PINs, etc.

Source: https://usa.kaspersky.com/internet-security-center/definitions/spear-phishing

Personally Identifiable Information (PII)

PII is any information about an individual maintained by an agency, including:

• Any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and

• Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Source: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf

Denial of Service (DoS) Attack

In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting your computer and its network connection, or the computers and network of the sites you are trying to use, an attacker may be able to prevent you from accessing email, websites, online accounts (banking, etc.), or other services that rely on the affected computer.

An attacker can use spam email messages to launch a similar attack on your email account. Whether you have an email account supplied by your employer or one available through a free service such as Yahoo or Hotmail, you are assigned a specific quota, which limits the amount of data you can have in your account at any given time. By sending many, or large, email messages to the account, an attacker can consume your quota, preventing you from receiving legitimate messages.

Source: https://www.us-cert.gov/ncas/tips/ST04-015

APPENDIX D: CASE STUDIES

Washington State Courts Data Breach

The Washington State Administrative Office of the Courts (AOC) announced in May 2013 that a security breach occurred on its public website as early as September 2012. No court records were altered and no personal financial information, such as bank account or credit card numbers, was stored on the site. However, other data stored on the server did include Social Security account numbers, names, dates of birth, addresses, and driver license numbers. Although there is no evidence confirming that any information was compromised, the data was vulnerable and considered as potentially exposed. Up to 160,000 Social Security numbers and one million driver license numbers may have potentially been accessed.

Once the breach was discovered, AOC took immediate action to further secure the environment and begin investigation and analysis into the depth and severity of the breach. In addition, AOC collaborated with the Washington State Consolidated Technology Services (CTS) and the Multi-State Information Sharing & Analysis Center (MS-ISAC) for internet security, who provided valuable information in determining the scope of this security breach.

The breach happened due to vulnerability in an Adobe Systems software program, ColdFusion, that has since been patched, court officials said. When court officials were first alerted to the breach, they believed all of the information accessed was public record, and did not think that confidential information was taken; however, after an investigation began, the broader breach was confirmed. Court officials said a law enforcement agency also investigated the case and concluded and there was no information on who might be to blame. Officials stated that the hackers were probably opportunistic and likely just fishing for data. Officials said that once the breach was confirmed, it took additional time to go through the files and increase security to the website, which is why there was a lag in notifying the public.

More information on the Washington State Courts Data Breach may be found at:

- http://www.courts.wa.gov/newsinfo/?fa=newsinfo.displayContent&theFile=dataBreach/commonQuestions
- http://www.courts.wa.gov/newsinfo/?fa=newsinfo.displayContent&theFile=dataBreach/home
- http://www.securityweek.com/server-washington-state-courts-office-hacked-sensitive-data-exposed
- http://seattletimes.com/html/localnews/2020956697_courthackedxml.html

Intrusion of Large Hospital Group Data Systems

A spokesperson from one of the biggest U.S. hospital groups confirmed in mid-August 2014 that its computer network was the target of an external criminal cyber-attack resulting in the theft of Social Security numbers and other personal data belonging to 4.5 million patients. The hospital group has 206 hospitals in 29 states. The attack is the largest of its type involving patient information since a U.S. Department of Health and Human Services website started tracking such breaches in 2009.

Working with a computer security company, the health group believed the attack was carried out by a group of foreign hackers that used "highly sophisticated malware" to attack its systems. The

intruder was able to bypass the company's security measures and successfully copy and transfer some data existing on the hospital group's systems. Security experts said the hacking group may have links to a foreign government. This group typically targets companies in the aerospace and defense, construction and engineering, technology, financial services, and healthcare industries, according to a member of the forensic team investigating this attack that occurred in April and June 2014.

The information stolen from this healthcare provider included patient names, addresses, birth dates, telephone numbers, and Social Security numbers of people who were referred or received services from doctors affiliated with the hospital group in the last five years, the company said in a regulatory filing. The stolen data did not include medical or clinical information, credit card numbers, or any intellectual property such as data on medical device development.

Since first discovering the attack, the hospital group has worked closely with federal law enforcement authorities in connection with their investigation of the matter. The company has implemented efforts designed to protect against future intrusions including implementing additional audit and surveillance technology to detect unauthorized intrusions, adopting advanced encryption technologies, and requiring users to change their access passwords.

This incident is one example of why cybersecurity has come under increased scrutiny at healthcare providers, both by law enforcement and attackers. The FBI warned the industry in April 2014 that its protections were lax compared with other sectors, making it vulnerable to hackers looking for details that could be used to access bank accounts or obtain prescriptions.

More information on the Large Hospital Group Data Systems intrusion can be found at:

- http://www.chs.net/media-notice-august-19-2014/
- http://www.cio.com/article/2466302/hackers-steal-data-on-45-million-us-hospital-patients.html
- http://www.reuters.com/article/2014/08/18/us-community-health-cybersecurity-idUSKBN0GI16N20140818

Home Improvement Retailer Payment System Breach

The world's largest home improvement retailer stated in early September 2014 that millions of credit and debit cards may have been compromised during a breach of its payment system. The retailer disclosed that cyber criminals armed with custom-built malware stole an estimated 56 million card numbers from its customers between April and September 2014. That disclosure officially makes this incident the largest retail card breach on record through September 2014.

The investigation into the breach began on September 2, 2014, immediately after the retailer received reports from its banking partners and law enforcement that criminals may have breached its systems. Since then, the company's IT security team worked with IT security firms, its banking partners, and the Secret Service to gather facts, resolve the problem, and provide information to customers. The investigation found evidence of compromise at approximately 1,700 of the nearly 2,200 U.S. stores, with another 112 stores in Canada potentially affected. There is no evidence that debit PINs were compromised or that the breach impacted stores in Mexico or customers who shopped on the retailer's online system.

Forensic investigators believe the attackers may have installed the malware mostly on the retailer's self-checkout systems. This finding could mean thieves stole far fewer cards during the breach

than they might have otherwise. Banking sources state that Visa and MasterCard have reported far fewer compromised cards than expected given the length of this retailer's six-month exposure. Multiple financial institutions reported that alerts from Visa and MasterCard about specific credit and debit cards compromised in this breach suggest that the thieves continued to steal card data a week after the breach was discovered and announced to the public.

Criminals used unique, custom-built malware to evade detection. The malware had not been seen previously in other attacks, according to the retailer's security partners. Forensic analysis revealed at least some of the retailer's store registers had been infected with a new variant of "BlackPOS" (a.k.a. "Kaptoxa"), a malware strain designed to siphon data from cards when they are swiped at infected point-of-sale systems running Microsoft Windows.

The analysis of the malware adds another indicator that those responsible for this breach may have been involved in the December 2013 attack on another large retailer that exposed 40 million customer debit and credit card accounts. BlackPOS also was found on point-of-sale systems at this retailer. Cards stolen from the home improvement retailer's shoppers first turned up for sale on Rescator[dot]cc, the same underground cybercrime shop that sold millions of cards stolen in December 2013 attack.

To protect customer data until the malware was eliminated, any terminals identified with malware were taken out of service, and the company said it quickly put in place other security enhancements. The "enhanced payment protection" involves new payment security protection that locks down payment data through enhanced encryption, which takes raw payment card information and scrambles it to make it unreadable and virtually useless to hackers. It also planned to deploy EMV Chip-and-PIN technology to U.S. stores by the end of 2014 as well as in its Canadian store network.

More information on the home improvement retailer payment system breach may be found at:

- http://www.bankrate.com/financing/credit-cards/home-depot-breach-bigger-than-targets/#ixzz3E0iJiYaD
- http://phx.corporate-ir.net/phoenix.zhtml?c=63646&p=RssLanding&cat=news&id=1969475
- http://krebsonsecurity.com/2014/09/home-depot-hit-by-same-malware-as-target/
- http://krebsonsecurity.com/2014/09/in-home-depot-breach-investigation-focuses-on-self-checkout-lanes/
- https://krebsonsecurity.com/2014/09/home-depot-56m-cards-impacted-malware-contained/

Hollywood hospital pays $17,000 in bitcoin to hackers.

Hollywood Presbyterian Medical Center paid a $17,000 ransom in bitcoin to a hacker who seized control of the hospital's computer systems and would give back access only when the money was paid. The assault on Hollywood Presbyterian occurred Feb. 5 2016, when hackers using malware infected the institution's computers, preventing hospital staff from being able to communicate from those devices, said Chief Executive Allen Stefanek.

The hacker demanded 40 bitcoin, the equivalent of about $17,000, he said.

The malware locks systems (CryptoLocker) by encrypting files and demanding ransom to obtain the decryption key. The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key.

Source:http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html

Identity Thieves Used Leaked PII to Steal ADP Payroll Info

Cybercriminals accessed a W-2 portal maintained by payroll company ADP recently to glean sensitive information about employees at a handful of companies.

The company is stressing that the company itself wasn't hacked, but that it appears identity thieves may have been able to create ADP accounts in the names of victims using previously leaked personally identifiable information. The problem ADP claims was a self-service registration portal that allowed attackers to set up fraudulent accounts in the names of employees at those undisclosed companies.

An investigation carried out by the company determined that attackers likely pieced together information on victims using other information published about them online. Any individuals who had their W-2 information compromised, likely had their information compromised previously, ADP claims.

Getting into the portal in the first place requires an access code unique to companies. ADP believes attackers targeted employees who had yet to sign up for the service. They gathered access codes from unsecured public websites of the companies and then either employees' dates of birth, employee numbers, or social security numbers, information that was either stolen via malware, or also published online, to gain access to the portal.

Source: https://threatpost.com/identity-thieves-used-leaked-pii-to-steal-adp-payroll-info/117842/

Office of Personnel Management Data Breach

One of the biggest hacks of sensitive information was the hack on the Office of Personnel Management (OPM). OPM detected a cyber-intrusion affecting its information technology (IT) systems and data. OPM estimated a total of 21.5 million people had their Social Security identification numbers and other sensitive information stolen in the hacking incident which occurred in April of 2015. Investigators ultimately determined that 19.7 million applicants for security clearances had their Social Security numbers and other personal information stolen and 1.8 million relatives and other associates also had information taken, according to OPM. That includes 3.6 million of the current and former government employees for a total of 22.1 million

"Protecting our Federal employee data from malicious cyber incidents is of the highest priority at OPM," said OPM Director Katherine Archuleta. "We take very seriously our responsibility to secure the information stored in our systems, and in coordination with our agency partners, our experienced team is constantly identifying opportunities to further protect the data with which we are entrusted." In addition to the 22.1 million social security numbers and sensitive information, 5.6 million finger print records were also stolen.

Sources:

- https://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/
- https://www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats/
- https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/

APPENDIX E: CYBERSECURITY DOCTRINE AND RESOURCES

Principal Doctrine

- Comprehensive National Cybersecurity Initiative (CNCI) http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative
- Cybersecurity: Authoritative Reports and Resources (Congressional Research Service) http://www.fas.org/sgp/crs/misc/R42507.pdf
- Cyberspace Policy Review http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
- Draft National Cyber Incident Response Plan (NCIRP) (2010)
- Executive Order: Improving Critical Infrastructure Cybersecurity (2013) http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
- Framework for Improving Critical Infrastructure Cybersecurity (2014) http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf
- Homeland Security Presidential Directive (HSPD 7) https://www.dhs.gov/homeland-security-presidential-directive-7
- National Institute of Standards and Technology Computer Security Incident Handling Guide http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf
- National Strategy for Trusted Identities in Cyberspace (2011) http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf
- National Strategy to Secure Cyberspace (2003) https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf
- Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (2013) http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

Department of Homeland Security

Cyber Capabilities/Entities

- National Cybersecurity and Communications Integration Center (NCCIC) (contact: NCCIC@hq.dhs.gov)
  - Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) (contact: ics-cert@hq.dhs.gov; 877-776-7585)
  - National Coordinating Center for Communications (NCC) (contact: NCC@hq.dhs.gov; 703-235-5080)
  - United States Computer Emergency Readiness Team (US-CERT) (contact: info@us-cert.gov; 888-282-0870)
- National Infrastructure Coordinating Center (contact: NICC@hq.dhs.gov)

Resources/Documents

- Cyber Storm III Final Report
  http://www.dhs.gov/sites/default/files/publications/nppd/CyberStorm%20III%20FINAL%20Report.pdf
- DHS Blueprint for a Secure Cyber Future
  http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf
- DHS Memorandum of Agreement with Department of Defense
  http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf
- DHS Quadrennial Homeland Security Review
  http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf
- DHS Strategic Plan Fiscal Years 2012-2016
  https://www.dhs.gov/sites/default/files/publications/DHS%20Strategic%20Plan.pdf
- Enabling Distributed Security in Cyberspace
  http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf
- ICS-CERT Incident Response Summary Report 2009-2011
  http://ics-cert.us-cert.gov/sites/default/files/documents/ICS-CERT%20Incident%20Response%20Summary%20Report%20%282009-2011%29.pdf
- National Infrastructure Protection Plan (NIPP) 2013
  http://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience
- National Response Framework (NRF)
  http://www.fema.gov/national-response-framework
- NCCIC, US-CERT, ICS-CERT Fact Sheets
  ICS-CERT: http://ics-cert.us-cert.gov/sites/default/files/DHS_CyberSecurity_ICSCERT-FactSheet-v8.pdf
- Protected Critical Infrastructure Information (PCII) Program Fact Sheet
  http://www.dhs.gov/xlibrary/assets/pcii/dhs-ip-pcii-fact-sheet.pdf
- Testimony of National Cybersecurity and Communications Integration Center Director Seán P. McGurk, National Protection and Programs Directorate, before the U.S. House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, "The DHS Cybersecurity Mission: Promoting Innovation and Securing Critical Infrastructure"
  http://www.dhs.gov/ynews/testimony/testimony_1302814781943.shtm
- Written testimony of Department of Homeland Security Secretary Janet Napolitano for a Senate Committee on the Judiciary hearing titled "The Oversight of the Department of Homeland Security"
  http://www.dhs.gov/ynews/testimony/20120425-s1-dhs-oversight-sjc.shtm

State Government

Cyber Capabilities/Entities

- Washington State | Office of the Chief Information Officer https://ocio.wa.gov/
- Washington Technology Solutions (WaTech) https://watech.wa.gov/
- Washington State Emergency Management Division, Cybersecurity Program https://www.mil.wa.gov/emergency-management-division/cyber-security-program
- MS-ISAC (contact: info@msisac.org; 518-266-3460)

Resources/Documents

- Call to Action: Cybersecurity and the States (National Association of State Chief Information Officers [NASCIO]) http://www.nascio.org/advocacy/current/NASCIO_Cybersecurity_Call_to_Action_Final.pdf
- MS-ISAC Charter https://msisac.cisecurity.org/about/charter/documents/MS-ISACCharter2013-03.pdf
- MS-ISAC Cyber Incident Response Guide: A Non-Technical Guide http://msisac.cisecurity.org/members/local-government/documents/FINALIncidentResponseGuide.pdf
- Robert T. Stafford Disaster Relief and Emergency Assistance Act http://www.fema.gov/media-library-data/1383153669955-21f970b19e8eaa67087b7da9f4af706e/stafford_act_booklet_042213_508e.pdf

Private Sector/Business

Cyber Capabilities/Entities

- Business Executives for National Security http://www.bens.org/
- Electronic Privacy Information Center http://epic.org/
- Internet Security Alliance http://www.isalliance.org/
- National Council of ISACs http://www.isaccouncil.org/
- Partnership for Critical Infrastructure Security http://insidecybersecurity.com/iwpfile.html?file=pdf13/cs09102013_PCIS_Proposal_Effective_Public_Private_Partnership.pdf

Resources/Documents

- Commonsense Guide to Cyber Security for Small Businesses (U.S. Chamber of Commerce) http://www.ready.gov/sites/default/files/documents/files/security_for_small_business%5B1%5D.pdf
- The Financial Management of Cyber Risk (ANSI and Internet Security Alliance) http://publicaa.ansi.org/sites/apdl/khdoc/Financial+Management+of+Cyber+Risk.pdf
- The Role of ISACs in Private/Public Critical Infrastructure Protection http://www.isaccouncil.org/images/ISAC_Role_in_CIP.pdf
- Verizon Data Breaches Investigations Report (2012) http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf