Global Information Assurance Certification Paper

Incident Response Exercise Planning
Be Ready – Be Prepared

GIAC (GCIH) Gold Certification

Author: Kurtis Holland, Kurtis.Holland@gmail.com
Advisor: Hamed Khiabani, Ph.D.

Accepted: April 7th 2014

Abstract

Computer Incident Response Teams (CIRTs or IRTs) is a key component in Information Security incident response just as Business Continuity planning and Disaster Recovery (BC/DR) teams are to the entire organization at the time of a business disaster. Effective incident response, just like BC/DR doesn't just happen - it takes careful planning and most of all practice. Incident response requires organization, training of key personnel, and systematic procedures; therefore conducting several test exercises annually are key requirements in order to properly access your organizations readiness to an actual incident. This paper will bring together multiple topics to refresh the knowledge and skills necessary for an effective Incident Handler, as well as offer insight to organizational management. Don't be the IRT that waits until called as that will be too late – be ready and be prepared.

1. Introduction

Cybercrimes and the annual costs incurred by business are on the rise year over year. The number of companies reporting data loss or data compromise continues to increase both from internal and external sources. As a company who has a major stake in ecommerce, or even traditional brick and mortar, you invest in technology and resources to protect your investment at the same time trying to maximize your return on investment (ROI), lower your total cost of ownership (TCO) and maximize your profits. The dilemma facing many a Corporate Information Officer (CIO) and Corporate Information Security Officer (CISO) is what should be the capital investment on Information Security technology and resources to lower your risk of data loss, but not over spend affecting your overall profitability.

So what are the impact facing corporations today? The results from a global study made by the Ponemon Institute, shows the costs, frequency and time to remediate cyber-attacks continues to rise. The average annualized cost of this cybercrime from the sample of U.S. corporations was $11.56 million, or a 78 percent increase from four years ago. (Ponemon, October 2013) In additions, remediation of the incidents has increased nearly 130 percent, with the costs to resolve a single attack is more than $1 million with time to resolve averaging 32 days. (Ponemon, May 2013) No longer is the trend just a few script kiddies hacking and playing with tools they've compiled or downloaded on the World Wide Web, the trends are showing organization, sophistication, and collaboration between multiple groups.

"The threat landscape continues to evolve as cyber-attacks grow in sophistication, frequency and financial impact," said Frank Mong, Vice President and General Manager, Solutions, Enterprise Security Products, HP. "For the fourth consecutive year, we have seen the cost savings that intelligent security tools and governance practices can bring to organization…" (Hewlett-Packard, 2013)

So what can an organization do to reduce their risk? The answer to some would be to recommend technology overkill, but most of us will address this with a balance of intelligent security tools, governance practices and focused training of team members.

Kurtis Holland, Kurtis.Holland@gmail.com

For others they start with a well-structured Business Continuity and Impact assessment of security risk on their critical business functions and then move into the policy, plan and process phase. Infrastructure risk can be greatly reduced with multi-layer, multi-tier security architecture; however that can only be touched upon briefly. What will follow is the focus on those governance processes surrounding Incident Response organizational training. The results are expected to be repeatable and measureable becoming an integral part to minimize the financial impact to a business when an incident occurs.

2. Incident Response Program

An Incident Response program will consist of several key components that are an integral part of your overall Risk Management program. Effective computer incident response teams (CIRT) have one major goal and that is to reduce financial exposure to business threats. The start of such a team is sponsorship by senior management with their commitment to provide the proper organizational structure, tools, and resources. Requirements for and incident response program can be found in government and industry regulations: HIPAA (section 164.308(6)(i)), GLBA (section 314.4(b)(3)) and PCI DSS (section 12.9) and ISO/IEC 27002:2005. (Beaver, Search Disaster Recovery)

There are three key elements to the Incident Response Program (IRP) that include the incident response policy, the incident response plan, and the incident response procedures. As part of the annual assessment of the CIRT team, it is a requirement to review each component to address any changes, incorporate new requirements, and to provide awareness to new management or team members. Each corporation will have similar goals and objective in their Policy, Plan, and Processes. The core focus will outline the basics for what is necessary for effective and efficient Incident Response.

2.1. Incident Response Policy

Incident Handling Policy will vary widely between companies, but they will all have key components in common. This will include the support of Senior Management, the scope and objectives of the Incident Response policy. It will address team organization,

communication methods, and how the team interacts with internal and external organizations. The policy establishes what is and what is and is not an incident and how the Incident Response Plan and Procedures are involved. The policy is not complete without an annual review and validation requirement to ensure compliance with all corporate and regulatory requirements are being met.

Diligent IRTs will periodically review the policy and ensure they are current in all the requirements in their response plans and procedures. Management structure in communications with law enforcement, media, regulator bodies, and customers may frequently change, so it is important to keep abreast of these in the event of an actual incident investigation. (NIST 800-61, 2012)

2.2. Incident Response Plan

In order to adhere to an Incident Response Policy, you must have a plan documenting steps that must be followed. This is often a high level flow of key tasks or milestones, with details processes and procedures that instruct various members of the IRT on their specific requirements for a given task. As with the policy, each plan may vary from organization to organization, but the plan's "battle rhythm" will need to include the following: (McCarthy, 2012)

- Senior Management sponsorship and approval
- Goal and Objectives for Incident Response
- Organizational structure of the various team members, their resource requirements and their rolls whether centralized or distributed among the organization.
- Communication process for internal and external entities
- Outline the Incident Response methods for each classified incident from the policy
- Metrics for evaluating effectiveness of team and process
- Annual review and evaluation process

Part of the annual review and training should access each section of the plan and adjust accordingly due to changes in policy or the threats facing your organization. Focus the plan template areas in order to recognize and respond to incidents, access

situation quickly, notify appropriate individuals and team members about incident, engage incident response team, and escalate organizations responses and communication based on severity. (Search Disaster Recovery, 2011)

2.3. Incident Response Procedures

To manage the Policy and the Plan you need documents outlining the technical processes and techniques used during an investigation. They may be in the form of short check lists, or forms or they could be outlining details in how to investigate specific threats and collect log data or evidence for later analysis. The procedures will be the most detailed and comprehensive part of the Incident Response program with the goal to establish systematic and consistent approaches for each and every incident. The training of the individuals responsible for various procedures increases with the complexity of the procedures and the technical environment.

Although each organization will vary on the specific procedures, here are a few that are necessary for managing risk and creating a consistent resolution to each event. Each should have the appropriate sponsorship of the senior incident response management and be reviewed annually or as necessary if changes during a 'lessons learned' or 'post-mortem' requirement. Typical procedures include, but are not limited to:

- Communication – both internal and external to your organization
- Escalation Notification
- Incident Tracking Forms
- Incident Reporting and Documentation
- Investigation Checklists by technology platform
- Remediation Checklists by Risk and Threat classification
- Security Information Event Management (SIEM)
- Evidence Collection and Handling "Chain of Custody"
- Forensics Investigation and Documentation
- Data Retention and Destruction
- Non-Disclosure Agreements

Most organizations will have specific Information Security Policy and Procedures covering most of these categories, and the IRT will be able to leverage and adapt these as necessary. Ensure this plan represents your organization and make it "our plan" not "your plan" (McCarthy, 2012)

2.4. Incident Response Phases

Up to now we have focused on the basic policy, plan, and procedures that governance the Incident Response team and their partner groups will use. Partner groups will involve IT Audit, Legal, Corporate Communications, Network and System Operations, Network and System Engineering, and sometimes 3rd parties (e.g. Information Technology Providers, Hardware or Software Vendors, etc.). All these team members should be operating under a Non-Disclosure Privacy agreement as they will often be exposed to potentially very sensitive information during the course of an incident investigate. They should all have read the Incident Response Policy, Plan and Procedures applicable to their department.

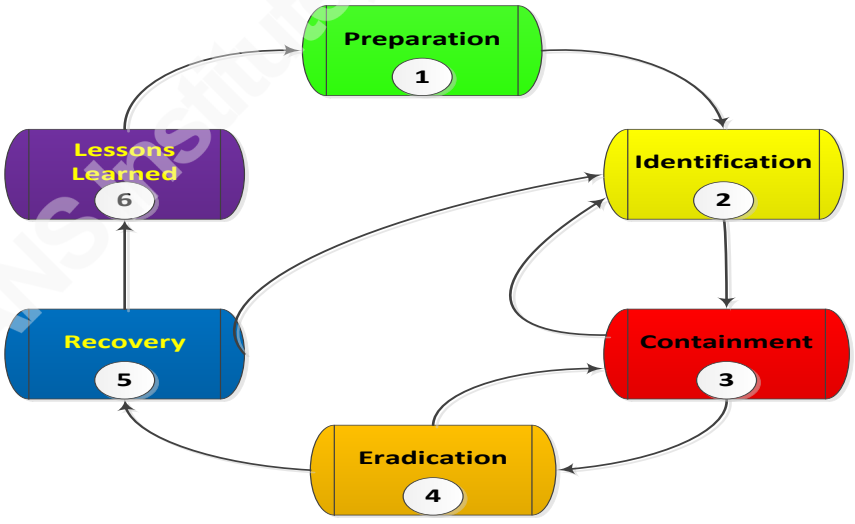

Figure 1 – Incident Response Life Cycle

It is important to next summarize the various phases in the Incident Response life cycle – the process of preparing for an incident, and then working through the various stages to identify, contain, eradicate, recover, and review lessons learned. (NIST 800-61,

2012) As you can see from Figure 1, a clean flow is not always possible, as before containment and eradication can be completed, additional issues arise and you have to continue the process until complete. Incident Response, like Information Security is a process – your review, remediate, revise, and repeat for each event.

2.4.1. Preparation

No one has ever written a completely secure program or designed a totally secure network so vulnerabilities do exist and they will eventually be found and exploited. There are numerous references to the 80/20 rule for Information Security based on Pareto Analysis, but you don't want to be blinded by the analysis. (Scott, 2010) It all comes down to proper assessment and risk management. No matter how much you harden or secure a system, "*Security is like a chain, it is only as strong as the weakest link*". (Schneier, 2005) You could spend millions on technical tools and consulting only to have it rendered useless due to an overlooked security control or human error. Preparation to handle incidents is not only the policy and plans discussed earlier, it is preparing your team with the proper procedures, documentation, and tools.

Several times per year, the IRTs need to update the inventory, usually with a checklist, on what should be maintained in their respective "jump kits", when they literally jump into action. Your communications plan, softphones, and escalation procedure will play an integral role getting this all started. It cannot be said enough that "Knowledge is Power" so ensure your process includes information threat intelligence gathering, software version levels, known exploits and malware, well-known ports and protocols, OS and Application software checksums, and current documentation on your network and systems security baselines.

Some organization will staff technical teams of first responders, and other will leverage 3rd parties or data center IT Provider and use an employee as the IRT lead and coordinator. In either case, the tools will vary as to your job role. Basic supplies such as laptop (Wi-Fi and Cellular enabled), notebooks, pen, paper, markers, smart phones, camera, portal printer, evidence bags, blank media, USB drives, labels, flash light, tool-kit, network hub, cables and power strip are used for a basic command center. (NIST 800-61, 2012) Some folks who have done this a lot would also recommend packing extra

clothes and personal hygiene supplies. All your policy, plans, procedures, checklist, and communication procedures need to be available both electronically and in print format.

Skills and tools to detect and analyze incidents is where most of the training and expense comes in. Digital Forensics workstations will support multiple versions of operating systems and often use virtualized guest operating systems with removable media for analysis. Not only will these systems have forensics analysis software, they will often contain network sniffers, protocol analyzers, software tools, vulnerability scanners and penetration testing software. And like all software, patch updates and new release maintenance will be an on-going challenge for the Incident Handler. These systems not only have to be secure, but they have to be accurate and reliable.

2.4.2. Identification

Incidents do not always say, "Hey you! Over here, did you miss me?" They are more subtle and may in your environment now for weeks or months before an anomaly is reported, often by a customer or an outsider. Locating and identifying some incidents and how they successfully attacked your environment is probably the most difficult part in Incident Response if you don't have the proper security architecture, baselines, and processes. Your Incident Handers also have to be prepared and trained to work with technical team members and know how to direct the investigation and handle the unexpected.

The modified tables below in Table 1 are examples summarizing some of the more common tools and methods to identify presence of an intrusion. Technology designed to monitor networks, application, and file systems for inappropriate content for both data at rest and data in motion. You need tools for logging transactions and results of security services. And to close it all off, services to track and monitor where the threat and attack vectors are coming from. (NIST 800-61, 2012)

Source	Description
Infrastructure Alerts	
IDS / IPS	Signature alerts or anomalous patterns, known attacks
SIEM	Event Correlation and log aggregation services
Anti-Virus	Malware detection of virus or phishing related files, Email
FIM	File Integrity Monitors detecting changes in file systems
3rd Parties	Fraud Services, Reputation Monitoring, Black Lists, DNS Fraud
Logs	
System	Operating system, Storage, Event and Accounting services
Application	Application services and database events and errors
Network	Firewall, Load Balancer, Switch or Router
Network Flows	Specialized data showing end to end session and connection detail
Public Information or Subscription Services	
Vulnerabilities	Common Vulnerably and Exploit web sites or subscription feeds
Hacker Sites	People outside who advertise tools and scripts for given software
Vendors	Believe it or not, some disclose vulnerabilities and patch data
People	
Employees	System Admins, Operations, or Developers often report incidents
Other Groups	3rd parties often notify Call Centers or Account personnel of issues

Table 1 - Intrusion Identification Attack Vectors

2.4.3. Containment

After a successful identification of the threat or vulnerability that was classified as an incident per your Incident Response Policy, it's now up to the IRT working with the appropriate groups to contain the threat. The IRT should have been diligence creating documentation of the incident, collecting evidence, assessing size and scope and looking into options to contain the impact is to the organization. A risk based decision will occur here with the Incident Handler and the organization. You either have a High, Medium or Low impact to deliver services, a potential data loss, or a combination. This is where the

communication plan and escalation process will become important as you advise the CISO and bring the business unit into the discussion. (NIST 800-61 2012)

There often is no standard response to each situation, so caution is recommended. Don't blindly filter traffic, stop a process or reboot your server(s) that are affected – follow your containment procedures for each type of platform validating the configurations, controls, and file systems. You may be able to achieve partial containment, as with vulnerability scans or low volume denial of service attacks.

Partial or full con containment by blocking offending attack signatures, E-mail or Web content through applicable filtering may be possible. Often you may never be able to fully remove the threat, but bring it to an acceptable level of tolerance. You are faced with the choice of "quarantine, or shut down", or "tolerate – live with the threat until eradicated". (McCarthy, 2012) Whatever your choice, make sure your containment strategy is aligned with your business risk assessments and the appropriate level of management makes the decision based on your advice on the risk and impact.

2.4.4. Eradication

This phase is where the IRT works with the appropriate network, systems, or applications personnel to address the incident. Evidence is gathered while correcting the problem ensuring that artifacts found within systems affected are removed. This could be patch updates, restoring file systems, adding network filters, removing inappropriate software, or even rebuilding the complete system. Ensure you follow a risk based approach and prioritize which assets are restored first based on the organizations business priorities. Validating the application, system, or network configurations post eradication is always recommend – both through visual inspection, automated tools, and vulnerability assessment techniques. The type of threat will have different forensics requirements, and in the case of malware, except for "zero day", signature and characteristics will be found in most threat and anti-virus database systems. (NIST 800-86, 2012)

2.4.5. Recovery

The time to get the application and services back online and into production will vary depending on incident impact to the organization and number of assets involved. This recovery is a prioritized and phased approach often coordinated with the eradication

phase. In some cases you may have to deploy a new technology or a service, such as with high volume DDoS attacks which will take weeks for procurement, deployment, and operational stability. In other cases, its coordinating patch updates to operating systems or applications. In the event of a Web application attack, correcting the software could take several months, and you'll have to deploy compensating controls with Intrusion Detection System (IDS) or deploy a Layer-7 firewall. Follow your process and checklist for bringing application online as you would a new deployment or install.

2.4.6. Lessons Learned

This is the closure phase of an incident life cycle where all the details of the incident is summarized and shared with the appropriate management and stake holders. This can be a very interesting an uncomfortable situation if the incident incurred a long remediation delay and large losses. What topics should be covered in lessons learned or incident post-mortem are:

- Incident Name
- Dates / Time and duration of the event
- Executive Summary
- Root Cause of the incident (the technical details)
- Who has been disclosed on the details of the incident
- What worked to assist identification, containment and eradication
- What improvements are recommended
- What are the next steps

As with all Incident Handling communications and reports, they should be tightly controlled, secured, and maintained for an appropriate period with evidence gathered according to your Incident Response Policy. The retention period should be adequate to meet appropriate statutes should the collected data be required in a prosecutorial lawsuit.

3. Objectives of the Exercise

The annual review of the Incident Handling Policy, Plan, and Procedures is similar to techniques and procedures outlined for other organizational IT Plans and requirements. The all have similar goals to evaluate the organizations ability to manage situations that arise with Information Technology. (NIST 800-84, 2006) In planning an annual exercise, as with Incident Handling, you will plan the exercise in phases. If from previous incidents, you had a weak spot or saw room for improvement, you might chose that item as the goal to evaluate in the exercise. If you know of an architectural issue or gap you want to document in more detail, what better way to show the gap then have issues occur during an evaluation of your IRP and procedures. After you work through the planned design of the exercise and develop the scenario you want to test, conduct the exercise and evaluate the results.

3.1. Identify Key participants for the exercise

Aside from the formal review of the Incident Handling Policy with senior management and the IRT management, the best was to conduct an IRP evaluation is to treat it as if it were an actually reported incident. As the exercise coordinator, you'll want to inform appropriate management an exercise will be conducted, but often not the details of the event. As shown in Figure 2 below, the Incident Handling Communications and Participants for a typical organization will include representation from Legal, Audit, Corporate Communications, Public Relations, Operations (System, Network, and Security), and Security (Physical and Information).

There is a preference to have the Incident Response management team report up through Information Security department to the Chief Information Security Officer. The CISO will be involved in all decisions communicating internal and external to the organization, briefing other organization executives, and overseeing the Incident Response plan. (McCarthy, 2012) In the case of extremely large corporations, they may be multiple Incident Response teams for each specialized line of business or geographical region due to complexities involved with international travel and language skills.

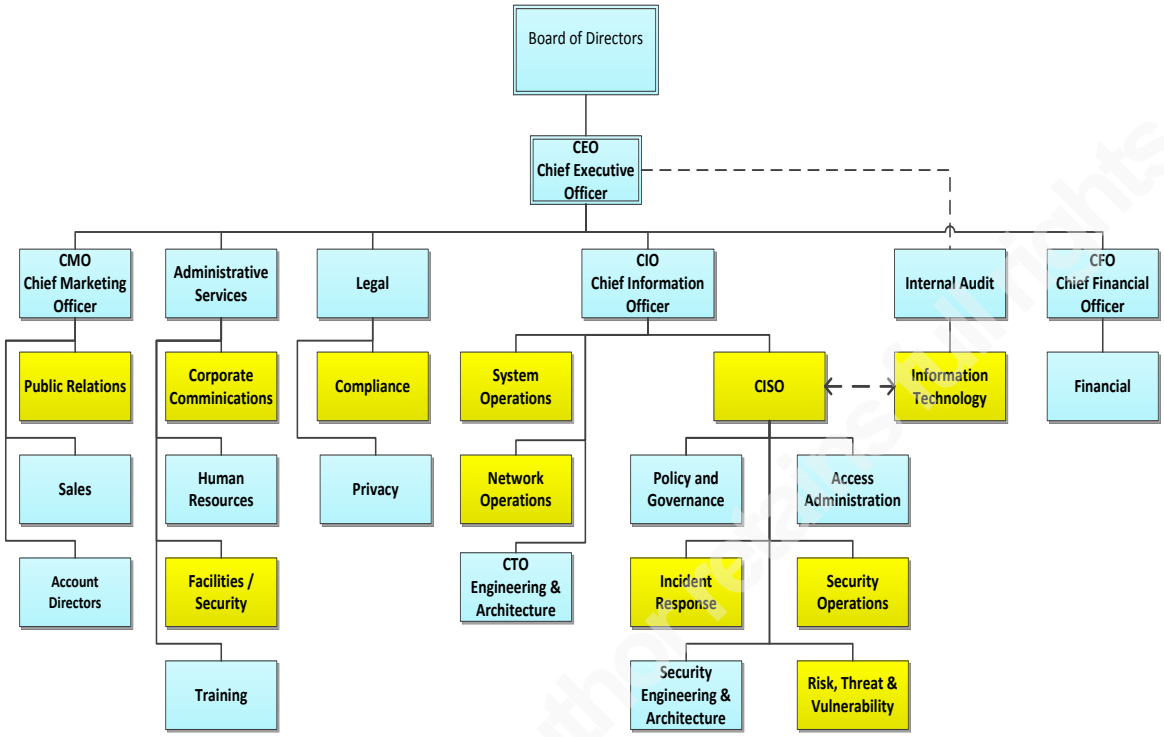

Figure 2 - Incident Response Communications and Participants

This is intended only to represent a possible organization with cross departmental participation with the skills and expertise required to handle and response to most incidents. Not shown are other Incident Response groups external to the company such as Service Providers, Forensics Consultants, Law Enforcement agencies, and so forth.

3.2. Annual Incident Response Policy and Plan validation

The Incident Response annual assessment can be broken down into two parts: 1) Policy and Plan review; and 2) Incident Handling Exercise and process review. For the policy and plan review, this can be done with a meeting with appropriate management. Once you brief the CISO, he or she can present that to other C-Level management and get their agreements. This review would cover changes in legal, compliance, notification, team members, incident classification, or communications. The following table can serve as a guideline or template for your annual review and planning, understanding each policy may not have the same section or order. (NIST, 800-61, 2012)

Kurtis Holland, Kurtis.Holland@gmail.com

Incident Response Policy Review Template		
Section Review Objective	Target Date	Completion Date
1. Executive Statement	MMM-DD-YYYY	MMM-DD-YYYY
2. Policy Overview	MMM-DD-YYYY	MMM-DD-YYYY
3. Scope	MMM-DD-YYYY	MMM-DD-YYYY
4. Organizations Structure & Roles	MMM-DD-YYYY	MMM-DD-YYYY
5. Incident Response Plan	MMM-DD-YYYY	MMM-DD-YYYY
6. Incident Identification & Severity	MMM-DD-YYYY	MMM-DD-YYYY
7. Communication & Reporting	MMM-DD-YYYY	MMM-DD-YYYY

Table 2 – Incident Response Policy Review Template

The review of the Incident Response Plan (IRP) will also be in two phases. First a manual review of the IRP for updates or changes as part of the management review. Each organizational stake holder should assess all components of the plan associated with their area. The second will be the actual Incident Handling exercise where the Incident Handling team performs the technical validation. Unfortunate organizations have a continuous process in the review and update of their IRP as they undergo multiple incidents per year. Some may go without significant incidents and this exercise will be beneficial to dust of the cobwebs. In either case, the following table will serve as a guideline for the annual review of the IRP. (NIST 800-61, 2012)

Incident Response Plan Review Template		
Section Review Objective	Target Date	Completion Date
1. Mission Statement	MMM-DD-YYYY	MMM-DD-YYYY
2. Plan Overview	MMM-DD-YYYY	MMM-DD-YYYY
3. Management Statement	MMM-DD-YYYY	MMM-DD-YYYY
4. Incident Response Process	MMM-DD-YYYY	MMM-DD-YYYY
5. Communication Plan	MMM-DD-YYYY	MMM-DD-YYYY
6. Measurement Metrics	MMM-DD-YYYY	MMM-DD-YYYY

Kurtis Holland, Kurtis.Holland@gmail.com

7. Roadmap & Review Requirements	MMM-DD-YYYY	MMM-DD-YYYY
8. Documentation & Reporting	MMM-DD-YYYY	MMM-DD-YYYY

Table 3 – Incident Response Plan Review Template

3.3. Roles and Responsibilities

The roles and responsibilities for the IRT members during normal incidents will be similar for the annual validation process. The dedicated Incident Response group will have the role of planning and coordinating the activity, pulling together the annual policy and plan review, and running the validation exercise. It is recommended at least all team members participate in one of the exercise validation scenarios, either the policy and plan reviews, or the actual incident simulation. Whether the team members are permanent or part-time participants to the main IRT, they need the appropriate skill sets and expertise in the area they will assist in. You do not ask Windows System Engineers to look at UNIX or Linux systems, and neither will they be involved with Network Routers or Firewalls. Putting members on an IRT is a significant management decision so it is important they are vetted properly for the proper skill sets and ability.

3.3.1. CISO and Senior Management

The IRT Director (or manager) often reports to the Chief Information Security Officer within an organization. The IRT lead oversees the various roles within the team, and provides the daily briefing to the CISO, so he/she can brief senior management. Per the organization example on Figure 2, representatives from Audit, Legal, Marketing, Public Relations, Security, Operations and Engineering make of the core management team. The actual Incident Team will not be the Directors or Vice Presidents in these respective areas but will often report to them with dotted line involvement with the permanent incident handlers in the IT Security group under the CISO as mentioned in the regional or international organizational approach.

3.3.2. Legal

Legal counsel is a necessary component on an IRT especially when it comes to researching and interpreting laws – both foreign and domestic. They provide guidance

when required to communicate with Government and Law Enforcement agencies. The Privacy and Compliance counsel will work closely with the Information Security Risk team. With 46 states now requiring data breach notification, it is important to review each incident to determine if disclosure of the incident is required. (NCSL, 2014) Legal also have so to keep us with the ever changing data breach statutes and directives from many national governments and the European Union which require notifications to appropriate regulator or national body within 24 to 72 hours. (WLG, 2013)

3.3.3. Public Relations

At one point in an organizations lifetime, it is going to be necessary to notify 3rd parties of an incident – either with a single customer, multiple customers, or even the news media. The will work with legal console in preparing a public statement or notification release. Many breach notification laws currently require notification when a loss of personal data in combination with other data such as Email, national identification, credit card, or health information. Of course, Public Relations may draft a notification, but will never release one without all the approvals from Legal and Sr. management carefully vetting the fact.

3.3.4. Incident Handlers

Incident Handlers are the core group in the team responsible for the execution of the plan and procedures when an event occurs. They are responsible in recommending the declaration an incident, providing a code name, and working the Incident Handling life cycle to identify, contain, eradicate and recover from the occurrence. Aside from keeping up with current threat and vulnerability trends, patch releases, OS fingerprinting; they will coordinate with other engineering teams and application groups during the investigation. The Incident Handlers will collect and maintain the evident during investigation, create daily summaries, and draft the final Incident Report for review with the CISO before formal publication within the organization.

The skill sets of the Incident Handlers will vary in their expertise of specific platforms and technology. Understanding all the details for various networks, servers, applications and the software component running on them is rarely found with one or two people. You most likely draft volunteers from the various organizations with that

expertise. In some cases, these personnel are involved with Penetration testing, with Network or System Engineering, Application Development, or other groups.

3.3.5. Security Operations

The Security Operations (SecOps) group within an organization is normally responsible for all the security tools used by applications as services. Parts of this team will monitor the security health of networks and servers with support Incident Handlers during the Identification, Containment, and Remediation phases of an incident. This team often overseas the operations numerous security services: Security Access (Directory, Radius/TACACS), Security Information Event Management (SIEM), and Intrusion Detection/Prevention, Anti-Virus, and File Integrity Monitoring infrastructure.

The SecOps will often run analysis reports to correlate events that are collected from various systems and applications to report on anomalies. They are often one of the first groups to detect and report an incident other than System Operations or Network Operations if a performance impact is not present (i.e. Denial of Service). Depending on the organization, SecOps may be integrated with the Network or System operations. The other variation is whether centralized or decentralized across the organization business units based on various business or regulatory considerations.

3.3.6. Operations

Operation groups have primarily one role and that is the management and monitoring of Network, Systems, and Applications supporting the organization and its customer base. This is most always a 7 x 24 x 365 process where the Incident Handling team may not have a direct contact on each shift to assist with sensitive incident investigation. There primary advantage to the IRT is their knowledge of the systems, the data flow, and the normal. The normal being what typically occurs on a given shift – the transaction volumes, type of jobs running, typical network and system capacity, and so on. In most cases, the IRT will enlist the assistance of one or two in the Operations group and have them on-call as needed.

3.3.7. Network and System Engineering

Engineering are the personnel the Incident Handler leverages when details of specific network or system configurations need to be validated. The support the configuration and patch management and have the necessary access to pull data necessary for analyzing that can lead to the identification, containment or eradication of the incident. They can apply temporary changes to configurations to change network flow, unmounts a disk volume for analysis, or to add additional capacity. The team and operations are integral in assisting the IRT as they have the necessary administration rights to the infrastructure that needs investigating.

3.3.8. Application Engineers

Application engineers are the team responsible for the development or deployment of commercial application services. The application was either written or purchased with integration into your environment by application engineers in the application development teams. When issues arise with log or event messages that cannot be explained, they will be the 2nd or 3rd level of support for the Operations teams. In a well formed software development life-cycle, they were involved in the testing, security assessments and hardening of the application and may be required to assist with detailed investigations depending on the event and threat.

4. Incident Response – Putting it all together

Any successful exercise begins with planning and preparation. To properly test a process used with incident handling, you need to develop checks that will validate the expected results when feeding invalid data into the system. To stress a weakness in the plan or uncover one that is not expected would be considered positive outcomes. Pick scenarios that 'think outside the box' and put the Incident Response team and supporting groups through their paces. Don't pick a simple IDS signature to block from an unexpected vulnerability scan – you are most likely getting hundreds or more per day. Don't pick a DDoS attack unless you want to combine with a transition to your Cloud or ISP DDoS service to test that redirect and vulnerability and threat scrubbing service.

Kurtis Holland, Kurtis.Holland@gmail.com

The recent Verizon Data Breach Investigation Report tells a historical tale of massive losses of personal data. According to Verizon, "…over the entire nine-year range of this study that tally now exceeds 2,500 data disclosures and 1.1 billion compromised records." (Verizon, 2013) Based on that information, the focus of at least one table talk exercise should deal with identifying the source of a data loss and what the potential root cause might be.

You exercise could be to investigate issues within your network, or one of your service provider networks. Your focus could be on a "Cloud" deployment where you are in a shared environment without full visibility and limited by what is part of the service offering. With the increase in Mobile Computing, you may want a scenario that investigates how you would manage a data loss with a compromised application design with weak encryption, segmentation or checks for compromised access privilege. Below is the process in Figure 3 that will be used to design the exercise scenario.

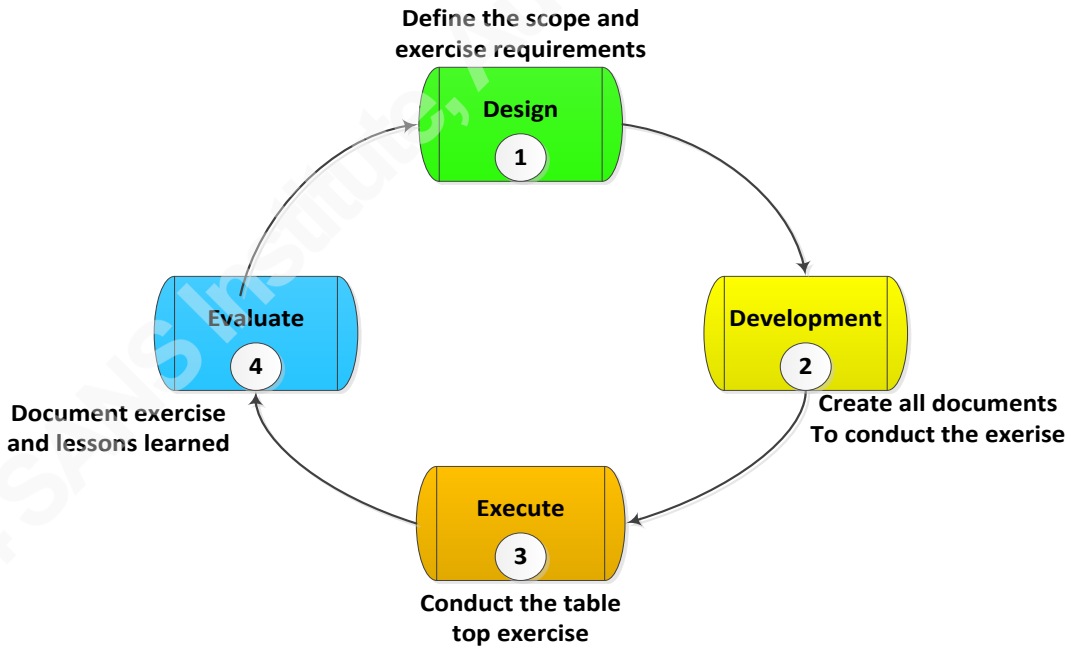

Figure 3 – Test, Training, and Exercise (TTE) Program Process (NIST 800-84)

4.1. Exercise Design

There are numerous use-cases to explore during your annual review of your IRP. The test will be short and focused, however in a real incident you don't know where it will

take you or how much it will end up costing in time and resources. With a paper exercise you have a clearly written process with orchestrated or random responses such as 'wildcards' or 'injections' to your normal flow. With today's cyber threats, I also recommend you spend time with an exercise scenario that allows you to evaluate the tools and infrastructure within your organization.

While you may wait five minutes in a table talk to receive and analyze logs discussing the process to request or generate a report – it may take hours or days in real-time. Launch that query and measure the response times, and include that in the final summary a few days after the exercise. The Exercise planning, design and development phase can either be individually created or split out and done as a team. Roles during the execution phase will have the facilitator, most often the Lead Incident Handler, and a scribe to take notes; record minutes, and document the results of the exercise.

As mentioned earlier, the overall policy and plan content is best reviewed and updated outside the exercise, just touching the highlights with the team if any significant changes occurred since the last review. A checklist for the plan Design and Development is shown in the following table below.

Incident Response Plan Exercise – Design		
Task	**Expected Date**	**Completed Date**
Establish Scope	MMM-DD-YYYY	MMM-DD-YYYY
Identify Exercise Objectives	MMM-DD-YYYY	MMM-DD-YYYY
Identify Participants & Exercise Staff	MMM-DD-YYYY	MMM-DD-YYYY
Identify meeting location and resources	MMM-DD-YYYY	MMM-DD-YYYY
Create the Exercise Documentation	MMM-DD-YYYY	MMM-DD-YYYY
Schedule Facilities & Phone Hot-line	MMM-DD-YYYY	MMM-DD-YYYY
Schedule Exercise	MMM-DD-YYYY	MMM-DD-YYYY

Table 4 – Incident Response Plan Exercise – Design

After the design of the test and training exercise for the IRP is completed, the team will then develop the scenario(s) they wish to validate. You want to ensure everyone

participates in the technical scenario. You may wish to keep the senior management policy and plan review to a simple one (1) hour or less review. For the actual exercise scenario team, you will include system and network operations, system and network engineering, security operations, security risk management, the Incident Handlers and the immediate management for escalation.

I especially like to have the CISO or a representative bungee jump in and out with injection of new data attempting to create a crisis. It is important for the Incident Handler and team to remain call, not get distracted, think outside the box, and be methodical in their approach making no assumptions. This will enable you to validate the IRP and procedures used by each area of the team. I recommend a formal approach to this review as it will be required for compliance, so the better the documentation the better the exercise will turn out. To development the scenario, the following example table can be used to serve as a guide: (NIST 800-84, 2006)

Incident Response Plan Exercise – Development		
Task	**Expected Date**	**Completed Date**
Create Exercise Overview / Presentation	MMM-DD-YYYY	MMM-DD-YYYY
Create Scenario Scripts & Participant Guides	MMM-DD-YYYY	MMM-DD-YYYY
Create Facilitator & Recorder Notebooks	MMM-DD-YYYY	MMM-DD-YYYY
Print Policy, Plan, and Procedures	MMM-DD-YYYY	MMM-DD-YYYY
Schedule Audio/Video & War Room	MMM-DD-YYYY	MMM-DD-YYYY
Create Management Notification Plan	MMM-DD-YYYY	MMM-DD-YYYY
Prepare targeted system reports to validate	MMM-DD-YYYY	MMM-DD-YYYY
Review Materials & finalize exercise date	MMM-DD-YYYY	MMM-DD-YYYY

Table 5 – Incident Response Exercise Plan – Development

A scenario that reviews the plan and procedures on paper is an excellent way to start the review. Your technical team will practice their detailed skills outside the exercise, in dedicated laboratories and facilities. The table talk exercise is all about communication and facilitating an investigation.

Kurtis Holland, Kurtis.Holland@gmail.com

4.2. Exercise Execution

Well, the big day is finally upon you. You conducted your management review of the Incident Response Policy and Plan and any revisions have been updated, and approved. Materials are prepared, reservations are made and you ordered coffee, donuts to entice participation. You may have spent a few weeks designing and developing the table talk exercise if this was your first time, but most of the material will be re-usable or work directly with normal investigations so this is not lost effort.

4.2.1. Exercise Rules of Engagement

The exercise should be conducted with several key tenets in mind. Do no harm to Production data and assets. I recommend you use this exercise to run sample queries on your tools and gather operational response metrics in parallel to the table top discussion. Everyone participates for his or her role with the appropriate process and procedures they will follow. You make sure each participant has an opportunity to evaluate the procedures associated with his or her area of focus.

With a pure table talk, you can discuss procedures, but you're not accessing any of the infrastructures to validate the tools, so to simulate responses, you can prepare a stack of index cards with expected answers or unanticipated ones that direct the scenario in one of several directions. For example if you ask how long it will take for a report, the answer might be we run one every night, so I can access it right now. If you ask what services are running on a server, the System Engineers card might say, "I don't know and it will take me an hour to compare baselines to what is running". A firewall engineer might be asked for a report on Layer 7 abnormal activity in the payment card environment, and their reply might be "Which ones, we have over multiple clusters supporting numerous demilitarized zones (DMZ)". As I mentioned, I am skeptical about performance of tools until measured under stress, so it is always a good practice to test these periodically just to understand response times and quality of information available.

Make this exercise both a technical and operational experience and it does not hurt to have a little fun in the process.

Kurtis Holland, Kurtis.Holland@gmail.com

4.2.2. Exercise Pre-Validation Checks

You cannot validate your technical and administrative procedures as part of a table top exercise; they are often way to technical and complex. Conduct pre-validation checks or tests to provide an operational baseline as to the team's readiness to response to an actual incident. The categories to assess and validate include: Component checks, System checks, and Comprehensive checks. (NIST 800-84, 2006) Prepare a checklist as part of the incident handling program for each team who is responsible to present current operational metrics as to the functionality of your 'defense in depth' capabilities of your deployed environment.

The test is a routine validation of the tools deployed that support both operations and security infrastructure. Formal documentation would include a report summary with:

- Name of Infrastructure Service
- Responsible Manager
- Team Members and contact information
- Description of Service
- Date Test Conducted
- Results (Metrics, or standard reports)
- Comments or Issues noted for remediation

Infrastructure will vary depending on the organization, and as to whether it is insourced or outsourced. Each component will have a policy and baseline configuration and an operational procedure for monitoring events and collecting and reporting on the resulting metrics. The components within the infrastructure most often deployed are represented in the following table:

Incident Response Infrastructure Exercise - Validation		
Infrastructure Component	**Expected Date**	**Completed Date**
Firewall Event Logging & Metrics (L & M)	MMM-DD-YYYY	MMM-DD-YYYY
Web Application Firewall (L & M)	MMM-DD-YYYY	MMM-DD-YYYY
Intrusion Detection/Prevention (L & M)	MMM-DD-YYYY	MMM-DD-YYYY

Kurtis Holland, Kurtis.Holland@gmail.com

Anti-Virus / Malware (L & M)	MMM-DD-YYYY	MMM-DD-YYYY
File Integrity Monitoring (L & M)	MMM-DD-YYYY	MMM-DD-YYYY
Domain Name Services (L & M)	MMM-DD-YYYY	MMM-DD-YYYY
Network Access Control (L & M)	MMM-DD-YYYY	MMM-DD-YYYY
Patch & Version Management (L & M)	MMM-DD-YYYY	MMM-DD-YYYY
Security Information Event Management	MMM-DD-YYYY	MMM-DD-YYYY
Network Monitoring Dashboards	MMM-DD-YYYY	MMM-DD-YYYY
System Monitoring Dashboards	MMM-DD-YYYY	MMM-DD-YYYY
Application Event & Error (L & M)	MMM-DD-YYYY	MMM-DD-YYYY
System & Network Configuration Baselines	MMM-DD-YYYY	MMM-DD-YYYY
Risk, Vulnerability & Threat Dashboard	MMM-DD-YYYY	MMM-DD-YYYY
Forensics Tools Validation	MMM-DD-YYYY	MMM-DD-YYYY
Critical Application Data Flow Diagrams	MMM-DD-YYYY	MMM-DD-YYYY

Table 6 - Incident Response Infrastructure Exercise – Validation

As you can guess, not all of these are the responsibility of the Incident Response team, but are key to assist in identification of an event, track it, contain it, and sure it remains remediation post eradication. Outputs of these components often trigger the escalation to the IRT, such as abnormal network or system behavior, detections of inappropriate files or processes, or a new threat where a patch or remediation may not be readily available in the case of 'zero-day' vulnerabilities.

4.2.3. Exercise Engage

Structure within the engagement will lead to better success in documenting what works and what does not. Ensure you are properly staffed to lead the meeting and have a designated facilitator for records keeping and gathering the materials validated for the final report. It is recommended that all the key participants are onsite during the exercise, but with technology, you can conduct audio/video presentations using products such as GoToMeeting, Live Meeting, or Webex according to your needs. This is only an exercise; however, if using an electronic meeting (eRoom) ensure appropriate security on

calendar invitations and meeting access. Utilize the agenda created during the design and development phases. You will already have shared prepared the materials, either physical or eRoom.

XYZ Corp Incident Handling Response Team

Validation Exercise - March 10, 2014

Agenda

08:30 – 08:45 a.m.	Introductions
08:45 - 09:30 a.m.	Exercise Overview (Goals, Objectives, Roles, Rules, etc.)
09:30 – 11:30 a.m.	Incident Response Plan – Table Top Exercise
11:00 – 12:00	Incident Response Plan Debrief

The Scenario (as listed by the facilitator) might go like this:

> "It was brought to our attention by two of issuing banks that numerous fraudulent credit card charges were made to customer credit cards that were used at our organization. We have a list of 100 cards from issuing bank and card ABC and another 250 from issuing bank and card DEF. So we have a report of 350 cards there were involved with fraudulent activity listing our organization as the potential source of this activity."

The facilitator now can use this scenario to help drive the review of the Incident Response Plan and the Procedures. Each person when queried could provide an answer to help guide the scenario, or respond using the queue cards provided for the script. So where to start…questions that may be asked of the team members to guide the initial investigation could include:

1. What is the classification of this event? If declared an incident, what is the severity per our Incident Response Policy?
2. Do we have any threat indications with our Operational monitoring of our critical applications?
3. Do we have any threat indications with our Security Monitoring components? (I.e. Anti-Virus/Malware, IDS/IPS, File Integrity Monitoring Tools, Risk & Threat Services, etc.)

Kurtis Holland, Kurtis.Holland@gmail.com

4. Have there been any significant changes in the Network or Payment Card environments?
5. Are we working any remediation on vulnerabilities found from our quarterly vulnerability scans or recent penetration tests?
6. Who will coordinate the investigation on a data loss report - the Incident Response Team or Fraud Team?
7. Do we need more information, like card numbers, dates used, etc., before we can proceed in the investigation?
8. What is our reply to the merchant acquiring bank processor or issuing banks and who should make it?
9. Where would you begin to look for an event of such small magnitude?
10. Once we validate we are the source of the incident, how long will it take to contain and eradicate?

So far, some of your team may be dozing off, if you did not bring coffee or other caffeinated beverages. But remember, you scripted some of the answers in cards before each team member and his or her role. The System Operations team declares this a "False Alarm", however, the CISO corrects this by stating this is a real event as we are the only common merchant in all the transactions reported fraudulent which is most likely statistically significant.

This scenario is time compressed and designed to take an unknown investigation duration down to a response of 24 – 72 hours to report or confirm a data loss to appropriate organizations and compress it to just under 90 minutes. As mentioned in the Development phase, you verified prior to the exercise that your security event and infrastructure management tools are operationally ready and procedures have been reviewed. You are also fortunate to have all your merchant network diagrams and application data flows. And if that is not enough, the System Engineering and Application teams have provided the configuration, patch, data flow, and network designs of your critical infrastructure. You have reviewed the Incident Response Policy with management, and both Legal and Public Affairs (Communications) are briefed on their role and procedures to follow. As a facilitator and Incident handler you are about to engage.

Kurtis Holland, Kurtis.Holland@gmail.com

4.2.4. Exercise Incident Tracking – Summary Documentation

As part of the Incident Response Plan you have created a process for documenting and tracking reported events that may rise to the classification of an incident. For this exercise you will be recording much the same information as you would should this has been an actual incident. Your internal communications would be identified, labeled, and properly secured such that only those with a "need to know" would be informed to avoid any further exposure outside official channels. If you have a computerized tool to do this, then that is excellent; however this short form can be used for tracking manually with appropriate attachments linked via document, spreadsheet, or uniform resource locator to your secure storage.

Incident Investigation Summary – "<insert Code Word assigned"		
Date	**Incident Summary**	**Key Actions**
Date / Time	Initial Report, "Event Name" • Document how you were notified of the event • Why was this brought to our attention? • Is this customer urgency? (H/M/L) • Assign incident codename (i.e. coded phrase) • Issue instructions on how to securely communicate and to restrict discussions outside the investigation team	List details of systems or networks under investigation
Date / Time	1st summary (or 2nd, 3rd, etc., add sections as appropriate) • Validate and clarify for misinformation • Points of contact (i.e. Customer, 3rd Party, etc.) with company name and phone numbers/time zones) • Information Requested (logs, IDS/IPS, A/V, FIM, etc.) • Resources needed (dataflow diagrams, application inventory, subject matter experts) • Internal escalations (who has been notified) • Next update or immediate actions	Update outstanding actions from a previous date/time
Date / Time	• Incident Handler/Incident Lead directs actions until no longer required • Document status, action items completed, next steps as required by Incident Handler/Incident Lead	Update outstanding actions from a previous date/time
Date	Weekly Accumulations - Key findings or changes week 1 should include: • Internal escalations • Possible causes or risks removed from current	

Kurtis Holland, Kurtis.Holland@gmail.com

	consideration • Logs examined (includes dates and system names) • Next actions (including external/customer communications planned and the rough schedule)	

Table 7 – Investigation Summary Template

So we are into initial notification and investigation for our table top exercise. There may not be a sense of urgency other than confirming data usage and which applications were involved to attempt to locate the data loss. You have a vague report to investigate, although you know your merchant acquirer networks and issuing banks do not report issues without probable cause.

The facilitator of the meeting will transition the running of the meeting to the Lead Incident Hander, and help coordinate the notes and record keeping. As fraud is involved, a lot of the team will stand down until more details on when and where the affected cards were used in XYZ Corp services. The basic information was recording on the Incident Investigation Summary as follows:

Incident Investigation Summary – "Spring Break"		
Date	**Incident Summary**	**Key Actions**
March 10th, 2013	Initial report date for XYZ Corp • Notified by Issuing Bank-X and Card ABC, John Smith, 214-555-1212 via Email of 100 Credit Cards • Notified by Issuing Bank-Y and Card DEF, Jane Doe, 817-555-1212 via Phone Call of 250 Credit Cards • Report of potential data loss and fraudulent use of Credit Cards • Notified John Johnson, CISO, and he contacted each acquirer to confirm Card Names, CC Pan, and Dates. Each vendor to send PGP secure file with Names, Dates. CC PAN, card type, and expiry date • Customer urgency is classified as High • Assigned Incident Code Name: Spring Break • Assembled Incident Response Team, Scheduled Bridge Call as this is a global operations team	Suspected Networks: • Payment Gateways • Web Portals • Point of Sale Network • Card Processing Infrastructure • Unknown

	• Notified IRT and CISO that this is a preliminary investigation and no further communications until next checkpoint	

Table 8 – Incident Investigation Summary – Initial Notification

4.2.5. Exercise - Investigation

We've now entered the first phase of the investigation, and the Lead incident Handler is meeting with the core team via a secure bridge (in this case in the Mock Exercise Conference room). The CISO, System Operations, Security Operations, Security Risk & Threat, Legal, and Engineering teams are in attendance with the IRT Lead and the IRT Technical Lead. They are briefed on the report and shared the results of the information received from the Acquiring Banks and it shows the cards in question were all presented for services at XYZ Corp between February 2nd and March 1st.

Like most fraud, it doesn't happen immediately but take time for the compromised data to be sold and inappropriately used. The acquiring banks and the card companies receive reports from their card holders, file the complaints, and conduct their investigations looking for common merchant usage.

The Lead Incident Response (IR) handler now asks each key member for a status of their environment, in the form of a roll call:

- System Operations reports no System Outages that were not scheduled for application or scheduled patch management.
- Security Operations reports no Anti-Virus Alerts, no IDS/IPS alarms other than normal Internet Scans that are blocked and shunted by the Web Application Firewall. Vulnerability scans (VA) by external Authorized Scan Vendor (ASV) show not Critical, High, or Medium findings. Internal VA scans are also clean. File Integrity Monitoring (FIM) dashboard is green for all card processing environments
- System Engineering reports Patch update status as current of last Operating System and Database patch releases. Application & Payment gateway servers are current as of December 31, 2013. No system capacity change after

shopping and booking capacity was added with 50 servers before the year-end freeze December 15th.

- Network Engineering reports all Firewalls, Switches and Load Balancers are current as of December 2013 patch releases. No network route or firewall changes except prior to the year-end freeze where additional capacity was brought online and we upgraded our Internet connections to 10 GB/s each with our two main ISPs at the Eastern and Western data centers.
- Security Risk & Threat reports status that no Zero-Day threats are reported; however there is a large spike in Spear Phishing and Malware affecting Windows environments….Threat Condition 2 and 3 depending on the A/V provider
- Payment Application Point of content brought in to ask about the status of the event and error log processing on the gateway systems to the card vendors. The report was no unusual system or network traffic.

Okay, so this doesn't offer much to the IR team. The CISO is worried about the response to his management and the Issuing Banks. The key here is not to reply before all the facts and details have been determined. It is too soon to start going through firewall, network and application logs until more details about access and usage is found. XYZ Corp is a Level 1 merchant processing more than 10 million credit transactions per month. The estimate from the Fraud team for a usage report is 4 hours to place the card usage to an application, date, and time. The Lead IRT also asks Security Operations to verify the WAF, IDS/IPS, and A/V policies for all the in-scope systems starting with the Web perimeter first. You draw a card, and their response is "2 hours for WAF and IDS/IPS policies but can't validate A/V until your tell us which systems to look at". So time elapses, and the team is reassembled to review data collected so far. In the real world, four or more hours would pass for validation of the cards in the booking database.

4.2.6. Exercise – Investigation First Summary

The team is now in full investigation mode to determine where and when in the reported credit cards were used in XYZ Corp. This will give an indication as to what

part of the data flow and which applications were involved. With Gigabytes of application log data per day per server and several hundred servers a detailed analysis of systems or their access logs is not practical in the early phase. Focus has been on the main booking database of record to determine if transactions with the questionable cards were used. 1st investigation summary might look like below:

Incident Investigation Summary – "Spring Break"		
Date	**Incident Summary**	**Key Actions**
March 10th, 2013 09:15	**1st Summary** "Spring Break" XYZ Corporation • Information received from Issuing Bank-X card ABC and Issuing Bank-Y card DEF on suspected data loss indicators • All Dashboards and Threat Indicators are Green – no operational or security alerts present • System Operations (First.Last@xyzcorp.com 555-1212) is running a report on master booking database to determine when and with what application suspected cards were used • Systems Security (First.Last@xyzcorp.com 555-1212) is verifying the IDS/IPS, A/V and FIM status on the core system for patch levels just in case we may be several weeks behind. • Engineering is pulling the application data flow diagrams for the four card processing environments in the regional data centers • No Internal escalations – CISO and Legal have been briefed • Next update schedule for 13:00 CST	Suspected Networks: • Payment Gateways • Web Portals • Point of Sale Network • Card Processing Infrastructure • Unknown

Table 9 – Incident Response Summary "Spring Break" – First Status

As far as some might think, this is just a false alarm or coincidence, but your CISO declared this an actual event. Time and your team marches on.

4.2.7. Exercise – Event Injection #1

The IRT is on standby pending investigation by the Fraud team. It is now about 11:30 CST in the morning and the Lead Handler is still awaiting first report and analysis of where the 350 reported cards were used. Enter the CISO, stage right, looking very

concerned and upset and just getting off a cell phone call. A new report just came from Issuing Bank-X card ABC upping their reported fraudulent count to 7,500 cards and they are getting calls on their help desk reporting fraud at an abnormally high rate. Another Issuing Bank-Z, with card HIJ, represented by Bob Bogus, 202-555-1212, called our CISO and reported an investigation they've been working on with the DOJ yielded approximately 25,000 of their issued cards found on an off-shore underground hacker site that sells stolen cards and their ongoing investigation shows the common usage at XYZ Corp within the last 3 transactions on the cards over the past four week period.

New information is now also reporting that the stolen cards have Card Verification Value (CVV) available. That's 32,850 cards total cards we could be liable for charge backs plus data loss notification charges. When asked about the fraudulent charges, it was reported that over $9,300,000 dollars to date in the first three months of this calendar year. It is beginning to look like a serious breach into your environment has occurred – either by internal or external means.

The Lead now calls Systems Operations and securely transmits the new list of cards to query. The lead waits for the Operations folks to call back confirming the receipt of the PGP Encrypted file exchange. As expected, all of the first 350 cards reported were used equally distributed with the web store fronts and the point of sale environments at the brick-and-mortar stores. This discussion on the new report and next steps planned with the CISO and System Operations pretty much took most of the lunch hour bringing it to the 13:00 CST meeting…time sure flies when you are having fun.

4.2.8. Exercise – Investigation Status Summary #2

The core IR team is now back on the conference call to review data collected and reviewed on the first 350 reported cards. With the notification of the additional loss of 32,500, with total charge-backs just over $9.3M dollars creates a hush during the meeting and on the bridge that seemed to last forever. The last data shared shows that all fraudulent transactions had CVV. The Lead notifies the team that evidence is pointing to systems in the Payment Service Gateway DMZ or network flow. Monitoring systems and tools are not showing appropriate security alert status. With all systems "Green",

which is very unlikely if there was a single or multiple compromise of a program, the focus now will be on what was missed or overlooked.

The Lead draws a card with the Payment Applications team, and confirms that the CVV is not stored post processing, so the vulnerability has to be in the data flow between the Point of Sale Servers or Cash Registers and the acquiring gateways. The Lead Handler also informs the team of the status of the FIM, A/V, IDS/IPS and patch levels appear normal through calendar end 2013….as to be expected due to current operational life cycle processes. The discussion among the team is now concerned we may had had alerts that were missed, vulnerability scans that missed an issue, or another threat that is not known.

The lead instructs his other handlers to put together a plan of assessment for the infrastructure. This involves hands-on validation of the key firewalls, application servers, and payment gateways looking for any anomaly. It is possible the Point of Sale at the brick and motor stores are at fault, but that is almost 50,000 Point of Sale nodes in over 1,000 stores. With the data loss report starting January 2nd, 2014, the team is looking now at system and log data from mid-November 2013 to year-end.

The Lead now recommends to the CISO to brief the Legal team and senior management about the 'non-disclosed' investigation, impressing the need for confidentiality, and begin preparations for potential ramifications and public notification, only when all the investigation data is in, as one of the acquiring banks has involved the DOJ. Investigation of servers and networks with no known alarms or alerts will take some time, so the Lead Handler tells the CISO the next briefing will be tomorrow or sooner if a significant finding occurs, but expect a full usage report for 17:00 today.

Incident Investigation Summary – "Spring Break"		
Date	**Incident Summary**	**Key Actions**
March 10th, 2014 13:00	**2nd Summary** "Spring Break" XYZ Corporation • Additional 25,000 possible fraudulent cards reported by Bob Bogus (202-555-1212) from Issuing Bank-Z cards HIJ. • Confirmed the first 350 were used between January 1st and February 1st 2014	Suspected Networks: • Payment Gateways Not ruled out • Web Portals • Point of Sale

Kurtis Holland, Kurtis.Holland@gmail.com

	• Issuing Bank-X card ABC upped their count to 7,500 • Plans for Engineering, Operations, and Sec Ops to inspect network, servers and data flow in / out of application and payment g/w starting 12-15-2013 • Next Mgmt. update at 17:00, technical follow up schedule for 13:00 CST, March 11th	Network • Card Processing Infrastructure

Table 10 – Incident Investigation Summary "Spring Break" – Second Status

4.2.9. Exercise – Pause for Reflection

What started as a routine investigation of potential fraud has now morphed into a much more serious event. This is a payment card data loss event, but it could easily have been a fire in the data center battery room; a massive denial of service attack, or a problem with your Cloud Service. With injections of additional data loss and law enforcement involvement at a 3rd party the investigation is now more serious and time constrained to resolve. With a compressed timeline to simulate hours and possible days for reports, you go about the investigation identification phase. In the real world, when working with dozens even hundreds of servers, this will take days for many of the lag analysis tools The Incident Team made some initial assumptions on where the problem is, but that is a starting point and you always plan the priority and the scope as manpower resources are always the limiting factor. We can begin containment or eradication, but if the source of the data loss is not found you may have to begin investigation or containment all over again.

Each team member using prepared procedures and automated tools to inspect the systems and networks to validate configurations and baselines. Network data flow analysis of logs and current traffic will hope to turn up an anomaly with the sensitive card processing environment. You are faced with a potential dilemma – you either have a false positive or signs of a significant breach with an unknown cause. The CISO and Legal briefing at 17:00 comes and goes with a brief status that reporting is progressing and analysis of the core systems is underway. Unless something turns up overnight, the next briefing is at 13:00 on March 11th. You draw another card.

4.2.10. Exercise – Event Injection #2

The team is now back in conference at 13:00 March 11th with nothing identified overnight. The Lead now asks the Sec Ops, Network, and Systems Engineering for a report on the Point of Sale systems and card payment gateways. He also queries the Applications team Fraud Team to pull data on all 32,850 cards on when they were used for sales and billing services. The results were not unexpected. So let us summarize briefly what they found in overnight investigations:

- System Operations and the Fraud team verified all the cards were used between January 2nd and March 8th, just over a 7 week period. A report with all the customer detail, include country, state, date, time, and where they were used.
- Network engineering found nothing out of the ordinary on the basic firewall and network traffic flow review prior to mid-December. Reports are still pending as for the end of December and January 1 – 7.
- System engineering inspected two of the four regional payment gateways, the two in the East Coast data center and so far all is normal. They verified all the binaries, libraries, configuration files with SHA-256 checksums. No abnormal processes, network connections or temporary files. They have just started to look at the other in the West Coast data center.
- System Operations has found nothing on the small sample of 100 POS terminals in 100 different stores. With 50,000 devices, a detailed analysis will take weeks if we cannot trust the A/V and FIM data.
- Security Operations verified several Alarms from the IDS and two from the FIM package that occurred on December 21st but do not appear to have appropriate closure information, but yet were flagged as 'false positives'. They draw a card and get lucky - they were on two of the gateways not yet inspected in the West Coast.
- System Operations draws there card and reports the uptimes for the two servers in question only date back to December 21st and the others back to November 15th when the quarterly patches were applied. This could indicate that two servers are now showing signs of a probable anomaly or undocumented change during the holiday freeze.

Kurtis Holland, Kurtis.Holland@gmail.com

Well, based on this information there appears to be some gaps in the System and Security Operations procedures as well as unaccounted for uptimes on two of the four payment gateways. What took just 24 to 36 hours in the simulation could have easily taking several weeks depending on the size and scope of your enterprise, where you started, state of your automation tools, and the number of assets to inspect.

There appears to have been an anomaly on December 21st, which was noticed but was not investigated and forgotten about. System monitoring of the processes didn't report the restart of two application services. It was just over a week later that fraud started to occur and no one notices.

Focus will not shift to the West Coast data center with the payment gateway environment where the update and IDS alerts were logged. All this technology deployed and the event appears to not have been addressed. The team will not overlook the server farm and databases used for the transactions, but focus will shift to the two remaining payment gateways as these are the only servers other than the point of sale or web gateways where all the CVV data flows through, and once transaction is authorized the CC Pan is tokenized and CVV is thrown away.

4.2.11. Exercise – Investigation Summary #3

Time passes quickly in a table top scenario. You are now more than 36 hours into this incident with several members of the team working long hours on 12 on and 12 off shifts. You have to continue pulling data for analysis and investigation. There are two servers with known issues and there may be others. Let's assume for tracking you got lucky and your System and Applications team found some very suspicious processes, numerous temporary files starting on December 21st, 2013 on the payment gateways that doesn't belong there. You now need to update your CISO and update current activity on your incident investigation summary.

Incident Investigation Summary – "Spring Break"		
Date	**Incident Summary**	**Key Actions**
March 11th, 2014 17:00	**3rd Summary** "Spring Break" XYZ Corporation • Network Engineering investigating firewall logs for data flow in and out of the payment gateway DMZ	Suspected Networks: • Payment Gateways

Kurtis Holland, Kurtis.Holland@gmail.com

	• System Engineering found Payment Gateway #1 and #2 with suspicious JAR files and running processes with what appear to be daily collection log files. Preparing to contain and analyze behavior of the rogue processes. • Security Operations is investigating a break down in the review process from December 21st where alarms on G/W #1 and #2 went unattended. • Additional Engineering teams continuing to inspect Payment Gateways, Web Portals, and Databases for malicious software. • CISO, Legal and Public Affairs have been briefed a confirmed malicious program was found on two of four gateway servers which appears to be collecting Credit Card data and shipping offsite – Name, Address, Phone, CC Pan, Expiration, CVV and in some cases PIN for debit cards. • CISO will provide a status update to each Bank Acquirer that the investigation is still continuing. No Public Affairs or Legal press notification at this time. • Next update schedule for 13:00 CST, March 12th	Not ruled out • Web Portals • Point of Sale Network • Card Processing Infrastructure

Table 11 – Incident Investigate Summary "Sprint Break" - Third Status

4.3. Exercise – Containment

Depending on your scenario, you could have injected more reports of fraudulent cards but that would essentially repeat more of the same reporting and usage investigation as already underway. The key now is assessing the damage done on the known servers, determine the scope of the data loss, and begin plans to eradicate the vulnerability, assuming the source of entry into the environment is found. You draw a card and your find it.

Depending on the size of your staff, you will also have to plan for how you manage a long investigation to meet the 24 – 72 hour reporting period. You may have to consider bringing in forensics consultants to analyze the type of attack and artifacts on the affected systems. Based on what is reported, the Lead Handler would most likely ask System Engineering what capacity is required for all the existing processing. To contain two servers, it may require adding more capacity to the environment if you want to error on

the side of caution, but you have adequate capacity to run on just two routing all the flow to the East Coast data center.

Before shutting any processing off, the system administrators are verifying system batch and startup file processes to ensure they have not been tampered with, and then suspend the application processing on these systems by taking them out of the load balancing pool. Your Forensics team draws a card, and this is a simple JBoss logger injected into the data flow. You can now shutdown or stop all the rogue processes at the same time with minimal risk of affecting the application processing. You collect all the evidence, change support and application passwords, and validate the system per your checklists.

Your system engineering should work with the forensics to preserve evidence to take a snapshot of the running environment, creating core files and capture mirrored drives to provide to the forensics team for further analysis, making copies of the images for evidence and to inspect for other issues than just the running process and deployed application from the inappropriate jar files. Your Security Operations team will need to determine root cause why the alerts of these changes went unanswered.

Incident Investigation Summary – "Spring Break"		
Date	**Incident Summary**	**Key Actions**
March 12th, 2014 13:00	**4th Summary** "Spring Break" XYZ Corporation • Network Engineering reviewing collected firewall paths to and from affected servers • System Engineering stood re-routed traffic to the East Coast why the two West Coast systems are being re-imaged. • Security Operations changing the Incident Monitoring process severity for the Application server deployment directory • Forensics is investigating mirrors taken on drives from two affected systems for further analysis • CISO, Legal and Public Affairs are preparing a contact memo to bank acquirer confirming the data loss which preparation for additional notification to law enforcement	Affected Systems: • Payment Gateway #1 and #2 • IT Provider Monitoring Server • Remote Access Server Clean environments: • Web Portals • Point of Sale Network

Table 12 – Incident Investigate Summary "Sprint Break" - Fourth Status

4.4. Exercise – Eradication

When moving into the eradication phase, your investigation and containment phases should have identified the key assets that are affected by this incident. For what we've discussed, you drew another card with Network Engineering and the only access to the console on the Payment Gateways is from the Management Network, and that monitoring service had access from your service provider's network. While your team is cleaning up your Lead brings in the service provider IRT point of contact into this discussion with full disclosure and notice of confidentiality. There must be a source of entry and exist into the network – either from a vulnerability in the network perimeter or from an internal system that was accessed remotely, i.e. malware through a proxy.

The System Engineers and Forensic team collaborated with the service provider IRT and found the ingress point and what the exploit was. Remote access via the Internet was available with a simple ID and Password. The lack of a two factor authentication, as this was a trusted partner, allowed them to establish a foothold as described on Table 11 using monitoring credentials and using open ports on the firewall to push data back out the entry path. Once on the maintenance network, they were able to use the captured credentials to look at other systems of interest to find the one monitoring the payment card environment. The traffic, although encrypted, was accessed using a valid password captured on the service providers monitoring server script as they were using non-encrypted storage of the credentials.

The forensics team identified the malware and a collection file containing every transaction processed from December 21st through March 12th when the process was stopped. Estimates are roughly 20 Million credit cards complete with Name, Address, Expiration and CVV from all the major card brands. No access to the database where the historical data was kept as this was a separate process not using the application server account. Drawing another card and this show is almost over.

The lead handler and the CISO now engage Legal and Public relations as it is there time to prepare for what follows post notification to the appropriate authorities, the issuing banks, and the DOJ that was brought into the investigation. You will try to make

the 72 hour notification window, but your legal counsel will make that call to report partial information of confirm the full scope of the data loss.

Incident Investigation Summary – "Spring Break"		
Date	**Incident Summary**	**Key Actions**
March 13th, 2014 17:00	**5th Summary** "Spring Break" XYZ Corporation • Operations restored on all four payment gateways • Remote Access server clear of all single use passwords • IT Provider rebuilding Monitoring server • Security Operations corrected IDS alert severity and added FIM monitoring of key directory • CISO, Legal and Public Affairs release press statement and letters to all Card Companies and Bank Acquirers. • CISO and legal preparing to meeting with Law Enforcement to turn over Incident details and evidence for follow up.	Affected Systems: • Payment Gateway #1 and #2 • IT Provider Monitoring Server • Remote Access Server Clean environments: • Web Portals • Point of Sale Network

Table 13 – Incident Investigate Summary "Sprint Break" - Fifth Status

4.5. Timeline

Summarizing the details of the exercise so far, you can see the extent of this exposure in that it was detected, preventable, but through human error went unreported and was not corrected until after the fraud reports started coming in. The Incident Response team is tracking this key information and you have it in a table format for extract into a tracking program or presentation. When writing up your summary report it would be appropriate to provide summary diagrams or data flows to illustrate the key point. A linear graphic with the key data points as shown in Figure 4 below emphasizes some of the key take away for remediating gaps in the security controls or procedures.

.

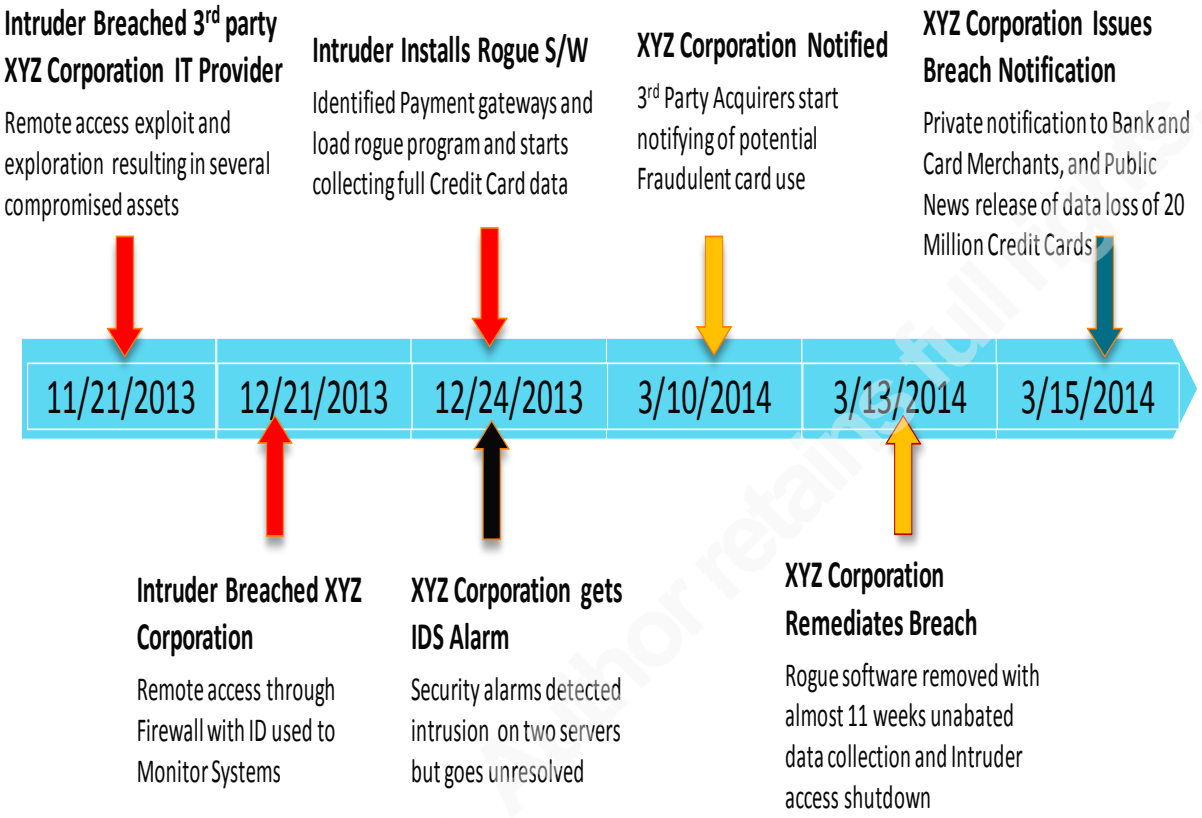

Figure 4 – Incident Investigation Summary Timeline

What is depicted below in Figure 5 below is a much simplified network data flow of the attack vector where the 3rd party breached an IT Provider network. Over time due to weak monitoring and captured credentials that looked like normal user access, the attackers found a path to where the XYZ Corp payment processing was going on prior to sending to the Merchant Acquiring Bank processors. The full CC PAN, Expiry Data, CVV, Card Holder Name and Address was all part of the data flow. Once the attacker had the credentials used to monitor the server and gain access to the JMX-console, they could push code to capture the data flow and move it back to their environment. The points of failure were the remote access, the malware to compromise access to internal systems, and then restarting the application server and it going un-noticed.

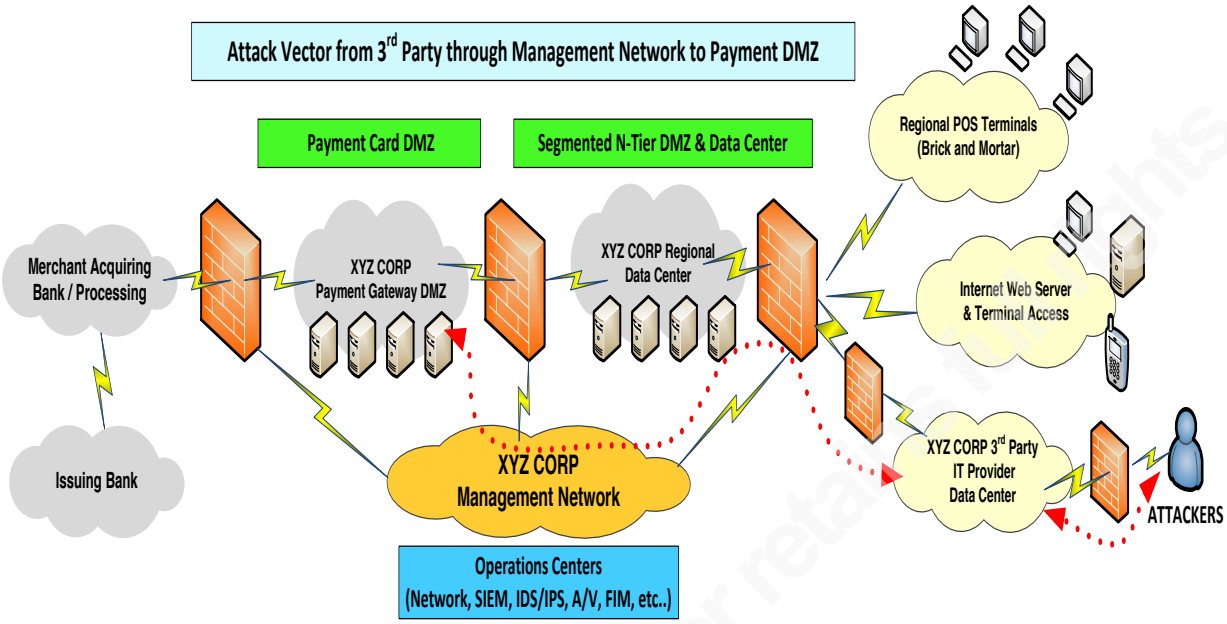

Figure 5 – Incident Investigation Summary Attack Vector Data Flow

5. Exercise Lessons Learned

For this exercise, the goal was to review the Incident Response Policy, the Incident Response Plan and Incident Response Procedures. The exercise facilitator guided the team through an exercise starting with a potential false alarm only to end up with a major data loss through inappropriate technical and administrative controls. There was a hidden agenda to this exercise as well due to all the recent network activity with Phishing, Malware, and attacks on various merchants.

Your CISO wanted to emphasize potential gaps in perimeter security, and some of the methods used to monitor applications with re-usable administrative passwords, not mutual authentication. To mix up the team, several injections occurred to put a stress of urgency on the event and to see how the team responds to intense external pressure. In lieu of this stress, you generated some real jobs to measure response and performance should a real need arise. After all you're not storing almost a petabyte of log and application data per year just to see how much floor space in the data centers it takes up.

So to summarize lessons learned:

- You learned to take Incident Handling requirements and break them down into the fundamentals and build a resilient and flexible team around them.
- Information Security and Incident Handling are processes – don't set them and forget them.
- Take advantage of scheduled audit requirements to stress suspected gaps or weaknesses in your security posture.
- Lack of two-factor authentication for administrative or remote access is a corporation's worst nightmare.
- Network security and access to private or shared environments are often outside your control.
- Do not assume all is well because you have operational and security dashboards all reporting normal activity.

6. Preparation of Exercise Closure Report

The Incident Summary and Tracking forms used during this exercise serve as useful data points and facts checks for drafting the Incident Report. You will archive all your collected evidence and retain it for the appropriate period of time to cover any follow up investigations or legal action. You will want to document a brief executive summary of the incident, the root cause, and recommendations to prevent or minimize impacts of a reoccurrence. It is well understood anything written down or e-mailed will be outside your control to secure access to it, so ensure it is properly labeled and classified as to the sensitivity and usage.

A more detailed report and investigation analysis will be created for the technical teams. Take special care to list evidence collected and how you tracked the chain of custody. Any communication outside the team needs to include not only the date and time, but who communicated and what the topic discussed was. Follow up the report with a summary of the issue and recommendations for next steps to reduce the threat of future incidents.

Kurtis Holland, Kurtis.Holland@gmail.com

7. Conclusion

This exercise was designed to provide the background in preparing an Incident Policy, a Response Plan, and how to validate your process and procedures. In this scenario, you started small and finished big with your entire team engaged providing their skills and expertise in the process. Incident response is an integral part of your information security and business continuity life cycles. It is difficult to manage your business technology risk if you do not formally asset the effectiveness of your Incident Response plan and procedures.

Incident Handling is not a subject to keep it small and make it simple. If you perceive or know of any gaps in your current infrastructure, stress those issue(s), document their risk if not remediated. In exercise planning, you do not assume all is well with your network and applications and that everyone did his or her support role without error. Information Security and Incident Response is a continuous process, not a "snapshot in time" that ends up as a checkmark on a compliance or audit assessment.

A successful exercise is one whom everyone participates and does not sit around drinking coffee, munching donuts, and telling stories of how they solved a past incident. Your Legal and Public Relations teams are not normally involved in minor incidents, but should be briefed annually should they need to be exposed to events involving regulatory and statutory response requirements. A large data loss is going to be a learning moment for all your senior management and board of directors. Keep your exercises flowing as you address the physical, technical and administrative requirements.

An exercise such as this one conducted in this paper resembles several of the recent data breaches reported by large and small corporations since 2005. (PRC, 2014) Some were insider threats, some were network intrusions, and some were human error. Many corporations had passed security assessment, but as the post-mortem analysis always tell, there were significant issues that were accidently overlooked. I believe Kris Herrin, from Heartland Payments systems said it best when he was quoted as saying "*Security leaders today need to assume their systems and networks are compromised and begin focusing on securing—or getting rid of—the data itself*". (CSO Online, 2008)

Kurtis Holland, Kurtis.Holland@gmail.com

8. References

Ponemon Institute LLC, (October 2013), *2013 Cost of Cyber Crime Study: United States*, Retrieved from: http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf

Ponemon Institute LLC, (May 2013), *2013 Cost of a Data Breach: Global Study*, Retrieved from: https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf

Hewlett-Packard Press Release, (October 2013), *HP Reveals Costs of Cybercrime Escalates 78 percent*, Retrieved from: http://www8.hp.com/us/en/hp-news/press-release.html?id=1501128#.Uw9yUYVDWRM

National Institute of Standards and Technology, (August 2012), *NIST SP800-61, Computer Security Incident Handling Guide, Rev 2*, Retrieved from: http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

National Institute of Standards and Technology, (August 2006), *NIST 800-86, Guide to Integrating Forensic Techniques into Incident Response*, Retrieved from: http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf

Scott, Charlie, SANS Institute, (2010), *Applying the Pareto Principle to Information Security Management*, Retrieved from: http://www.sans.edu/research/management-laboratory/article/mgt421-scott-pareto

National Institute of Standards and Technology, (September 2006), *NIST 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, Retrieved from: http://csrc.nist.gov/publications/nistpubs/800-84/SP800-84.pdf

Kurtis Holland, Kurtis.Holland@gmail.com

Beaver, Kevin, Search Disaster Recovery, Tech Target, *The importance of incident response plans in disaster recovery*, Retrieved from: http://searchdisasterrecovery.techtarget.com/tip/The-importance-of-incident-response-plans-in-disaster-recovery

Search Disaster Recovery, (Jan 2011), *Incident Response Plan Template*, Retrieve from: http://cdn.ttgtmedia.com/searchDisasterRecovery/downloads/SearchDisasterRecovery_Incident_Response_Plan_Template.doc

McCarthy, N.K & Todd, William, MacGraw-Hill, (2012), *Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk*, Retrieved from: http://www.amazon.com/Computer-Incident-Response-Planning-Handbook/dp/007179039X#reader_007179039X

Verizon Enterprise Solutions, (April 2013), *2013 Data Breach Investigations Report*, Retrieved from: http://www.verizonenterprise.com/DBIR/2013/

National Council of State Legislators (NCSL), (January 2014), *State Breach Notification Laws*, Retrieved from: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

World Law Group, (2013), *Global Guide to Data Breach Notifications*, Retrieved from: http://www.theworldlawgroup.com/files/file/WLG%20Global%20Data%20Breach%20Guide-Final.pdf

Privacy Rights Clearinghouse (PRC), (2014), *Chronology of Data Breaches, Security Breaches 2005 to Present*, Retrieved from: http://www.privacyrights.org/data-breach

Herrin, Kris, CSO Online, (2008), *Heartland Payment Systems CTO Kris Herrin talks about the attack that changed his views on data security*, Retrieved from: http://www.csoonline.com/article/701650/apt-in-action-the-heartland-breach

Kurtis Holland, Kurtis.Holland@gmail.com