justin greis

CASE STUDY: INCIDENT RESPONSE AND CYBERSECURITY

STOP, SHOP, AND ROLL, INC.

ASSIGNMENT OVERVIEW

Summary:	As a team, present the proposed solution to the case. The presentation should lay out clear recommendations for how management should address the problem. This case study is divided into two parts: 1. determining how to best respond to a cybersecurity breach within the first two weeks of the incident, and 2. analyzing and evaluating the company's cybersecurity capability and making recommendations on how to improve it, which occurs roughly two months later. Each team should analyze both parts of the case but only one team will present each part. You only need to turn in the deliverables for your assigned part of the case.
Presentation Deliverable:	Case study presentation (in Microsoft PowerPoint format)**.**
Executive Briefing Deliverable:	Single page case study executive briefing (in Microsoft Word format).

BACKGROUND

Stop, Shop, and Roll, Inc. (SSR) is a new company formed from the merger of three retail giants:

1. *Stop-n-Save* – Originally founded as a "dime store," Stop-n-Save evolved into a retail powerhouse appealing to a new generation of young buyers. They specialized in clothing, home goods, and a variety of other everyday convenience goods. Their main competitors were Target, Marshalls and TJ Maxx.
2. *Shopology (aka Shopology.com)* – Shopology carried overstock and out of season items purchased from premium retailers at deep discounts and sold those goods online. Prior to the merger, Shopology had no brick-and-mortar presence; they were a "pure play" online retailer. The main competitors of Shopology were: Target.com, Amazon.com, and Overstock.com.
3. *Roll With It* – Roll With It began as a roll-away bed company and quickly expanded into home furnishings and décor. They stocked mid- to high-end furnishings, furniture and home goods. Roll With It competed head-to-head with Ikea, Dania, Ashley, Toms-Price, Macy's and a few other home and department stores.

In 2014, the three companies came together under a new name – *Stop, Shop, and Roll* – in order to combine their collective strengths of mass appeal (Stop-n-Save), an online presence (Shopology) and the logistics and supply chain power (Roll With It). The merger garnered a lot of attention and excitement from Wall Street and company shareholders alike. The stock of the newly combined company soared as they launched their media and branding blitz. Expectations were high about the synergies each company would bring to the table but skeptics doubted managements' ability to deliver on the pre-merger promises. Nevertheless, the newly streamlined management team pressed ahead and committed to a quick and efficient post-merger integration of the over 5,000 combined applications innumerable processes. Was SSR up to the challenge?

THE NEW COMPANY: STOP, SHOP, AND ROLL, INC.

Once the afterglow of the merger activity wore off, management went to work on the integration of the three entities. Before the merger, the plan was for each company to run independently for one year while systems and processes were combined, data was migrated and people were realigned to new departments and positions. The plan was approved and sounded good to the newly formed board of directors. SSR even planned to leverage a "best of breed" strategy for its processes while standardizing on an all SAP platform: if one company had a best-in-class process, SSR would adopt it and use that as the global template in their global SAP instance. While the plan made sense in theory, SSR spent hundreds of millions of dollars on a transformation that lasted 3 years and seemed to generate more complex processes than before; certainly not the synergies they had initially planned.

After the third year of the over-extended transformation, a new CEO (Scott Farkus) was brought in to get the company in order. He completed the SAP project but each company ran its own instance with their own customized template. The processes were all different but did consolidate up to a centralized general ledger and few shared financial processes. The global instance of SAP failed to deliver the synergies but the company could finally operate as one organization with three business units:

1. Home
2. Furniture
3. Online

It took four years but SSR was finally one combined company. Although stock prices fell during this time (mainly because expectations around the cost savings, synergies and integration were so high), revenues were up and consumer response to the new brand was very positive. SSR looked like a very different company than the pre-merger company and was now a $25 billion company with 90,000 full time employees and 750 stores operating in the US, Mexico, Canada, Russia, Argentina, China, Japan and UK.

SSR IT AND THE CYBERSECURITY PROGRAM

The business transformation had been very tough on SSR Information Technology. IT had been blamed for the failure of the SAP unified global template and still carried a black eye for failing to deliver the synergies of the streamlined application portfolio. During the four year transformation, three CIOs rotated in and out of SSR. A recent New York Times report highlighted the successes and failures of the three SSR CIOs and examined why each leader was brought in and was ultimately fired. The fourth SSR CIO (Jason Piggott) entered the scene just as the final pieces of the transformation puzzle came together. Piggott, in reality, had little background in IT; he was an accountant turned brand manager who made a career leading technology-heavy projects (e.g. customer portals, mobile apps, and e-commerce websites). Piggott was a

dynamic, likeable leader but had little attention for the details of the job. He knew he was there to finish the job and get IT humming after a long arduous journey.

SSR IT

Piggott organized Information Technology into two primary functions:

1. Run the business
2. Transform the business

The "run the business" arm was composed of all the groups necessary to keep the business going in a steady state. Functions such as IT operations, infrastructure, telecommunications, cybersecurity, IT help desk/service management, and disaster recovery were among the operational IT functions that kept the business going. The "transform the business" was composed of organizations such as: IT program management office (and the associated projects), application development, product development, and enterprise architecture. Piggott was fortunate to have strong leaders in the IT functional areas, and despite his lack of formal IT training, Piggott was exceptionally good at solving problems and was respected throughout the organization for his ability to bring the organization together and get IT operating as a cohesive team.

Early in his organizational design, Piggott took a bold stance that he would embed the security function in every department. This decision received a lot of scrutiny and push-back from the management team and the board but Piggott convinced them, based on his experience, that it was the right thing to do. He appointed a Director of Cybersecurity, Jean Simmons, despite his peers' advice to create a Chief Security Officer (CSO) position and establish a dedicated department. Piggott believed that "security was everyone's responsibility" and having a CSO may relieve others' responsibility for securing their products and processes. Simmons was given the directive by Piggott to "publish policies and standards for how the organization should conduct secure business and everyone will follow them." Cybersecurity was established as a governance and oversight organization with only one person covering all security-related responsibilities of a global $25 billion company. Simmons had no dedicated security staff who reported to her, and after one month on the job, she began to see signs that all was not right.

SSR CYBERSECURITY HISTORY

The SSR cybersecurity department grew out of the seeds planted at the three companies:

1. *Stop-n-Save* – The "IT security department" primarily focused on protecting the credit card information of its customers. The department built a compliance-driven program very concerned with maintaining PCI (Payment Card Industry) compliance. While Stop-n-Save was generally acknowledged as a secure company, the reality was its staff was overly-focused on compliance versus maintaining a secure environment. The security department grew out of its internal audit group and had built comprehensive control matrices to track compliance and controls but often failed to address some of the more emerging threats that jeopardized their customer's sensitive information.
2. *Shopology* – Opposite of Stop-n-Save, Shopology took security very seriously. The former CISO (Chief Information Security Officer) of Shopology was former Air Force and believed strongly in maintaining command and control of his technology environment. Every aspect was locked down and monitored by a dedicated team of in-house security experts. The Shopology security operations function was a team of 60 dedicated security professionals who monitored the website

for bad activity, investigated incidents and responded rapidly to events. Shopology was even featured in KrebsOnSecurity.com and several other industry journals as one of the most effective and cutting-edge corporate cybersecurity teams.

3. *Roll With It* – Roll With It viewed security as a "necessary evil" function that was not core to their business. They managed security within their IT Operations group but, in reality, it was just a set of outsourced vendors. Roll With It personnel within IT set policy while Dell Secureworks managed everything else via a managed serves arrangement. Roll With It never really got involved in the details of how security was run; it was happy just knowing that it could set the policy and Dell Secureworks was enforcing it and monitoring it.

The plan was the three security organizations would come together during the merger and operate independently for the first year (like the rest of IT) and then start to make changes to align to the new operating model. But the first SSR CIO (John Harrington) became impatient and began to make changes in the first quarter of the newly formed company. Harrington slashed headcount at Shopology and Stop-n-Save as part of a cost-savings measure as he viewed them as "unnecessary overhead." Harrington believed that any non-core IT functions eroded margins; Harrington was ruthless about the slashing heads and getting rid of positions in the name of cost-savings.

When the second CIO entered the picture (Frank Kowalski), additional cuts were necessary to focus resources on the global SAP initiatives. Frank cut the Dell SecureWorks contract and folded monitoring and incident response functions into the former Shopology team's scope for protecting the environment.

The third CIO (Elizabeth Hynes) made minimal changes to Kowalski's design and let the organization run as-is for a year. However, Hynes left after just a year because she accepted a COO position at a competitor. Jason Piggott, SSR's fourth and final CIO, decided that cybersecurity needed more streamlining and moved all remaining security technical personnel into the IT operations group and made the appointment of Jean Simmons to the Director of Cybersecurity. Piggott directed Simmons to establish policies and standards and hand them off to the IT operations group to enforce and run.

CYBERSECURITY MODEL, STANDARDS, AND FRAMEWORKS

Simmons came from a very technical cybersecurity background and knew that a good foundation for cybersecurity must be put in place for a business to be successful. She knew that all successful cybersecurity departments followed a framework that enabled companies to:

1. *Complicate* an attacker's ability to achieve their objective.
2. *Detect* the attack before business impact is accomplished.
3. *Respond* and remediate effectively and efficiently to an attack.
4. *Educate* your workforce to create a security-conscious line of defense.
5. *Govern* the program by establishing a continuous and sustained improvement, clear accountability and executive oversight of the program.

In her past jobs, as long as these five components were in place, Simmons felt comfortable about the security program. The problem was: she did not believe that all the essential elements were in place. Simmons was accustomed to programs that followed standards like ISO27001, ISO27002, NIST800-53 and COBIT but that seemed to be missing at SSR. In fact, when Piggott instructed Simmons to start building standards, she was surprised that standards didn't already exist.

Simmons sought guidance and met with colleagues at the RSA Security Conference in San Francisco, California. One of her fellow CISO friends, Brian Clayton, handed her a framework that he had just

implemented called the CPM (Cyber Program Management) framework (see Exhibit One). Clayton explained that each aspect of the framework represented a key capability that all security functions had to have in place to be effective. Of course he recognized that not every organization executes these capabilities as well as others so each capability can be measured in terms of its maturity (see Exhibit Two for maturity scale definitions). Clayton also gave Simmons a copy of his CPM maturity model so that she could evaluate her organization in terms of its relative maturity. Simmons was grateful for this information and knew that she could directly apply this framework, together with the standards she had used in the past, to design an improved organization and future vision for cybersecurity at SSR. She just had to make the case to Piggott that it was worth the investment.

As Clayton and Simmons said goodbye, he handed her one final document. Clayton said:

> *"Remember, it's not a matter of IF you will get hacked, it's about WHEN and WHAT YOU WILL DO when it happens. Hearing what you have just told me about SSR, I would be surprised if the bad guys aren't already inside your network. I hope that's not the case!"*

Simmons gulped and unfolded the piece of paper Clayton handed to her. Clayton explained,

> *"This is a framework for responding to cybersecurity incidents. It has served me well many times. Like most companies with valuable information, we are constantly under attack and it is important you think through this model before a security event graduates to a major security breach."* (See Exhibit Three for Clayton's security incident response framework)

Simmons thanked Clayton and immediately went back to her hotel room to start compiling her observations about SSR so far.

GAPS IN THE CURRENT CYBERSECURITY PROGRAM

Back in her hotel room, Simmons immediately began writing a list of her observations about the SSR cybersecurity program. Each observation represented a major gap in the program. She paid close attention to the CPM framework but did not map her observations to the framework; she figured would have time to do that later. Below is the list that Simmons wrote:

- No formal information security strategy exists. No strategic plan has been created to map out what projects and key initiatives will be executed and when each will start and finish.
- Policies and standards exist but are selectively enforced; there is no formality around which policies are enforced and how effective SSR is at enforcing the policies and standards.
- The PCI compliance program is disconnected from the security program. A team of PCI professionals make sure SSR is compliant but they are not integrated with any of the people who manage operational security.
- Security monitoring is conducted by IT operations personnel. IT operations group focuses on making sure the systems stay up and running and most times do not have time to focus on investigating security incidents. They usually just reimage a server and move on.
- SSR does business with vendors and third parties without any sort of investigation or analysis of the security of that vendor.
- There is no centralized asset repository. SSR has spreadsheets (that are out-of-date) that detail all the assets (both software and hardware) it has. These spreadsheets do not contain any information about the applications or data assets; just the software and hardware for licensing and lease renewal purposes.

- There is no formal incident management process. IT operations usually handle all incidents but focuses on restoring services in any way they know how.
- SSR manages identities in each of the individual systems it uses. They have Active Directory for network identities, authorization and authentication as well as an SAP HR system that tracks all employee information; however, none of the applications are integrated. Users typically have to remember between 5-10 different username/password combinations for all systems.
- Simmons is not aware of any security-specific logging, alerting and event management function. She believes this could be one of the contributing factors to IT operations' lack of effective security incident management.
- There does not appear to be a comprehensive business continuity plan in place. In fact, Simmons was astonished that, with such a sensitive supply chain and retail network, SSR would not have some kind of business contingency plan in place. Funnily enough, no one could explain to Simmons what would happen if various parts of the business went down and were forced to recover. Most people she asks just shrug and say "we'll manage through it somehow."
- Reporting to executive management is ad-hoc and very difficult since there are few real security metrics that are maintained. The only metrics Simmons could find relate to IT operations SLAs (Service Level Agreements) and service effectiveness ticket metrics.
- Simmons has no staff and no one, except her, dedicated to the cybersecurity function. She also has very little budget. Simmons reviewed the budget from the last few years and noted SSR's average annual spend of $100,000 for security improvement initiatives ranging from antivirus improvement to purchasing additional network intrusion devices.

The list of security gaps could have gone on but Simmons ran out of hotel stationary (and also began to get a little worried). She started typing up her observations but knew that the message to Piggott had to be very tactfully worded and carefully crafted. Being a Friday, Simmons decided to write up an MS PowerPoint presentation over the weekend and send to Piggott first thing Monday morning.

THE HACK

THE DISCOVERY

Monday morning started out as any normal morning for Scott Farkus. He entered his office, booted up his PC as he normally did and immediately saw this image flash in front of his screen:

Farkus first thought it was a joke and called his executive assistant and said “Oh, ha ha…enough games. You know better than to mess with me on a Monday…” His assistant said she had no idea games Farkus was talking about but she couldn’t really talk right now as she was dealing with a computer problem. Farkus asked what the problem was, and to his horror, she described the screen Farkus was looking at.

Unable to email or use his PC, Farkus immediately picked up the phone and dialed Piggott. Piggott had not made it into work yet but had already started receiving calls about some mysterious virus going around the SSR machines.

Farkus got Piggott on the line and asked him if he knew what was going on. Piggott told Farkus that he was five minutes away from the office and would start investigating right away. Farkus described that the application holding his PC hostage looked like it was called “Cryptolocker.” Piggott said “That’s not good. I don’t know much about it but I know it’s a form of “ransomware” that typically requires we pay a designated amount of money or our files are deleted.”

Farkus started to get worried and upset. “Deleted!?!?!” he screamed. “What do you mean deleted?”

Piggott reassured Farkus, “we will be fine. I am pretty sure we can recover from this. Let me give Jean Simmons a call and we will get right on this.” Reluctantly, Farkus hung up and began walking around the executive suite where the CFO, COO and CMO sit. All of them had booted up their machines and were greeted with the same ominous screen.

Piggott knew the situation was bad. In fact, it was very bad; much worse than he had conveyed to Farkus. Piggott had been on calls with the IT operations command center since 4:00 AM about this issue. All of the Windows-based SSR servers had been infected and they were not sure how they were going to recover the information and restore service. Luckily, despite the corporate computer systems being infected, it did appear that the retail stores were untouched and seemed to be OK.

It was now 7:15 AM and employees in the US would begin to arrive at work in 45 minutes. Piggott knew he had to act fast. As soon as he hung up with Farkus, Piggott immediately dialed Jean Simmons’ mobile number and prayed that she would pick up.

THE CALL NO ONE WANTS

Simmons hadn’t slept well all weekend. The worry from her list of cybersecurity gaps kept replaying in her head. But, Simmons had a renewed sense of energy from the conference and knew she could formulate a plan to get the SSR cybersecurity function to where it needed to be. She knew a list of security gaps would not be well received by Piggott so spent the weekend formulating recommendations to address each gap. Simmons was proud of the ideas she had come up with and planned to get up extra early on Monday so she finalize her PowerPoint slides and could catch Piggott before his normal Monday morning schedule.

Simmons arrived at the office at 6:00 AM and received a call at 6:15 AM from a private/blocked number. She thought this was unusual and knew she had to focus and finalize her presentation so she forwarded the call to voicemail.

By 7:10 AM, Simmons was done writing up her summary slides and was ready to make her way into Piggott’s office. Simmons noticed she had a voicemail from the private number so she picked up her phone and hit play:

> *"Hello Ms. Simmons. This is Sheila Leonard from your regional FBI (Federal Bureau of Investigations) office. I'm not sure if you remember me but we met a while back at one of our business outreach meetings."*

Simmons did remember Leonard and immediately felt a rush of nerves in the pit of her stomach. Simmons carefully listened to the rest of the message:

> *"Ms. Simmons, the purpose of my call is we have reason to believe Stop-Shop-and-Roll has been the victim of a serious security breach. Our intelligence network has discovered over five million customer records, including transaction details, names, addresses, credit card information and more being sold on the black market. We have reason to believe the perpetrators have much more information they intend to leak and use for criminal purposes. We would like to discuss this matter with you immediately. This is extremely urgent and time is of the essence. Can you please give me a call back at (800) 555-2600? Thank you, Ms. Simmons."*

Stunned by the news, Simmons looked up at her finely crafted PowerPoint presentation she just completed. "How ironic," she thought. Clayton's voice echoed in her head: "Remember, it's not a matter of IF you will get hacked, it's about WHEN and WHAT YOU WILL DO when it happens."

"What should I do? How should I respond?" Simmons thought. Still shocked from the voicemail, Simmons thought "I better call back Sheila Leonard and find out more information. That way I can go to my management with all the facts on-hand."

Just as Simmons was about dial Leonard's number, Simmons received an incoming call. Her caller ID read: Jason Piggott. "How convenient," Simmons thought, "I can tell him about the call from the FBI and then call back Leonard for more information."

Simmons pressed the "Accept Call" button with a calm "Good Morning, Jason."

Piggott replied, "I'm not so sure this is such a good morning, Jean. Are you in the office yet? I think we have a problem."

YOUR TASK FOR THIS CASE – PRESENTING TEAMS

PART 1: INCIDENT RESPONSE

Create a plan of action for SSR to respond to the security breach. It is critical you address what needs to be done and the steps that need to be followed. You should leverage a framework for responding to the incident and carefully detail out the tasks for each phase of the framework. Be sure to indicate who needs to be involved at each phase of the response plan. A RASIC chart may help to show the tasks and the people who are involved at point in the response process. Your response time line should cover the first two weeks starting at the discovery of the hack. As usual, cost and resources are important so be sure to describe how much this will cost and how many resources this will take to address the problem.

PART 2: CYBERSECURITY PROGRAM IMPROVEMENT

After two months, the security incident was fully addressed but now it is time to up-lift the cybersecurity function. Examining the facts of the case, your team should come up with a plan to raise the capability maturity of the SSR cybersecurity function. You must propose recommendations that address the root cause issues of SSRs problems. Simmons and Piggott recognize that these changes cannot happen overnight so they would like to see a multi-phased plan for addressing key issues over the course of two years with key milestones and capability improvements delivered every quarter. Just as above, please include cost and resource estimates with your plan and recommendations.

WORKING TOGETHER

The groups working on parts 1 and 2 may, but do not have to, work together to solve this case. Because there are two separate presentations, each team's solutions are not required to be coordinated; however, you may decide to do so if you choose.

YOUR TASK FOR THIS CASE – ALL OTHER TEAMS

CASE STUDY EXECUTIVE BRIEFING

Given the incident's potential severe impact to SSR, an emergency Board of Directors meeting has been arranged. Farkus and Piggott have been requested to brief the Board of Directors on the incident and they only have 30 minutes. The Board of Directors want to know what the incident is, what the potential impacts are, what SSR is doing about it, when SSR expects to resolve the incident, and who is involved in the response. Farkus and Piggott want to provide a memo to the Board of Directors prior to the meeting so the Board can come prepared for an effective discussion. Given Farkus and Piggott don't have technical knowledge or incident response experience, they have asked your team to put together a single page executive briefing memo in Microsoft Word format.

GENERAL CASE STUDY GUIDANCE

At a minimum, the solution to your case study should include the criteria below. Though not mandatory, you may use this as a format and general flow for your case study.

- A clear and concise background of the facts of the case.
- Key issues, observations and complicating factors that contribute to the root cause business problem at hand.
- A clear statement of the business problem to be solved.
- An overview of the solution and its components. The solution should address the key tasks outlined for you in the case.
- Demonstration of sufficient analysis that led you arrived at your solution.
- Clear recommendations for how the solution should be implemented or deployed.
- A timeline for execution of your recommendations.
- A budget or cost model for implementing your solutions. Be sure to include the cost to build and deploy your solution and the cost to run and operate your solution after it is built.
- An analysis of the risks, issues, key assumptions and any mitigating factors you will employ to minimize the likelihood and/or impact.

You have been asked for a lot of detailed information to solve this case. The trick will be to package this up into a digestible executive presentation your audience can understand. Detailed supporting information can be included in an exhibit in the appendix of your presentation.

Your case study solution should also include:

- Citation of key sources in the form of end notes cited in your appendix.
- Application of standards and leading practices that help to inform your solution.

A few tips and tricks for solving this case:

- Company financials have intentionally not been provided to you for this case. To build your model about sizing of the company, please conduct your own independent research and find similar peer companies.
- Feel free to make assumptions that support your conclusions. Be sure to state your assumptions in an exhibit in your appendix. Your assumptions should not significantly alter the facts of the case; rather, they should support the recommendations by filling in the missing pieces of information in the case.
- You should NOT simply copy/paste from COBIT or any of the other standards. The key is to use the standards to help you solve the case. Remember: standards are NEVER the answer on their own; they must be applied to the business problem.

APPENDIX

EXHIBIT ONE: CYBER PROGRAM MANAGEMENT (CPM) FRAMEWORK

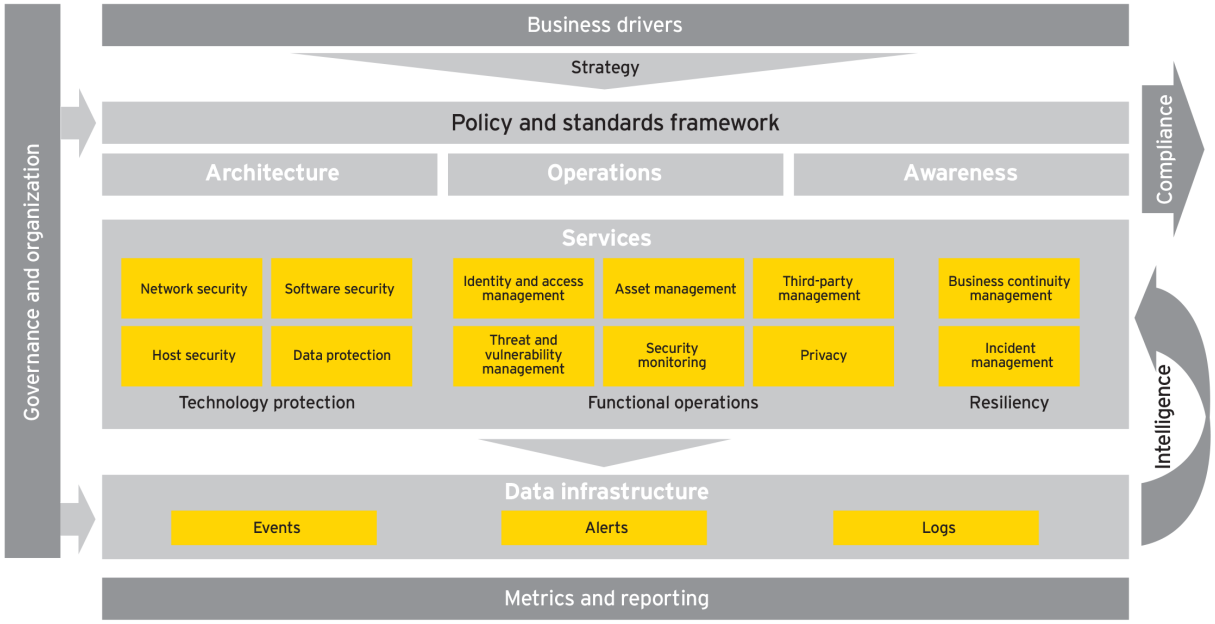

EXHIBIT TWO: CPM MATURITY MODEL DEFINITIONS

Rating	Definition
1	**Initial** Basic, ad-hoc, undocumented; changing capability may be in place with some technology and tools; limited local processes; limited organizational support.
2	**Managed** Partial capability is in place with a combination of some technology and tools; local processes covering some regions/business units or processes are repeatable but may not be good practice or maintained; limited organizational support to implement good practice.
3	**Defined** Defined capability is in place with significant technology and tools for some key resources and people; processes defined for some regions and/ or business units; organizational guidance and support is in place for some key regions and/or business units.
4	**Quantitatively managed** Mature capability is in place with advanced technology and tools for most key resources and people; consistent processes exist for most regions and/or business units; some governance is in place (accountability/responsibility/metrics) for most key regions and/or business units.
5	**Optimizing** Advanced capability is in place which is leading-edge technology and tools for all key resources and people; consistent process across regions and business units; effective governance is in place (accountability / responsibility/continual monitoring for improvement).

EXHIBIT THREE: SECURITY INCIDENT RESPONSE FRAMEWORK