Cyber Security Cookbook for Practitioners

Devesh Mishra
Technologist – Mount Sinai Health System, NY
New Jersey, USA
e-mail: dkm2144@columbia.edu

***Abstract*—The scope of this paper is to provide the essential framework to C-suite/Management executives in the case of cyber events. This paper will further analyze the various threat vectors from the operational perspective and provide the remediation plan during the case of cyber-attacks.**

Keywords-Component; (CIO; CISO; CFO; Risk Management)

I. GENERAL OVERVIEW

Organizations prepare for various types of emergencies by developing a disaster recovery plan to cover flood, fire, earthquakes, and other unforeseen events that may disrupt their operations. It is important to protect the organization's assets against cyber threats and having a robust playbook as well. According to IBM's CEO, "Cyber Crime Is the Greatest Threat to Every Company in the World"1. Darkreading.com states, "Global cost of cybercrime predicted to hit $6 trillion annually by 2021"2.

Cybersecurity should be an integral part of corporate strategy. As Touhill advises, the cybersecurity plan focuses on the following (Touhill & Touhill, 2014, as of Page 97):

- Where are we now?
  - SWOT analysis
- What do we have to work with?
  - Information
  - Technology
  - Finances
  - Personnel
  - Plans
- Where do we want to be?
  - Value
  - Risk Management
  - Effectiveness
  - Competencies
- How do we get there?
  - What will be done?
  - Who is responsible for doing it?
  - How will it be done?
  - What resources are required?
  - Risk Management
  - Measuring progress and success

The basic security principles of Least Privilege, Defense in Depth, and Separation of Duties are observed. These concepts will drive many of the security design decisions, just like Confidentiality, Integrity, Availability, and Accountability will inform the requirements for controls to mitigate specific risks. (Wheeler, 2011, Page 19).

II. ENTERPRISE RISK MANAGEMENT

Risk Management is defined as "the function of determining the proper steps to manage risk, whether it be to accept, mitigate, transfer, or avoid the risk". (Wheeler, 2011, Page 149):

- Accept: A decision to accept the risk
- Avoid: Ceasing (or not engaging in) the activity that is presenting the risk altogether
- Transfer: Shifting responsibility or liability for a risk to another party by contracting the corresponding cyber insurance
- Mitigate: Limit the exposure in some way

A. Risk Management and FAIR

Risks are identified and managed in accordance with corporate strategy and the corporation's risk appetite (Wheeler, 2011 Chapter 3 as of Page 43). Risk management incorporates the following:

- Resource Profiling
- Risk Assessment
- Risk Evaluation
- Documentation
- Risk Mitigation
- Validation
- Monitoring and Audit

The Factor Analysis of Information Risk (FAIR)3 is used as a model for understanding, analyzing and

DOI: 10.21307/ijanmc-2019-063

quantifying information risk in financial terms and builds a foundation for developing a scientific approach to information risk management.

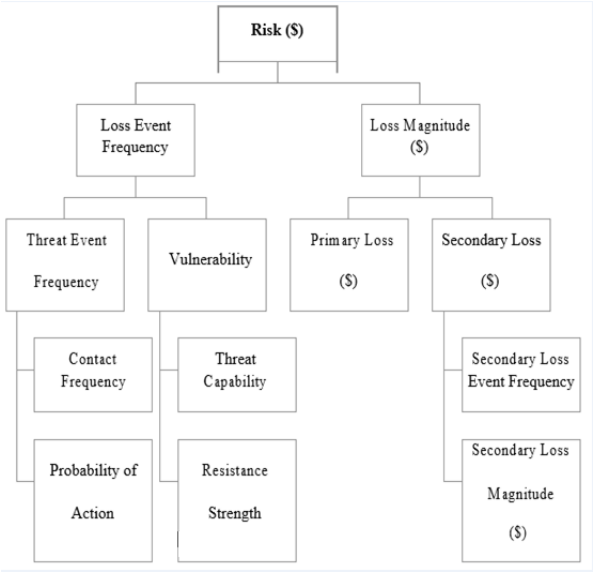


Figure 1. Factor analysis of information risk

For resource profiling, all resources are identified and the level of sensitivity is defined for each. A detailed threat analysis is performed quarterly to identify exposure and quantify risk and security controls are defined and implemented. It classifies the likelihood and consequences associated with each risk and how that risk could impact the business (See Tables 1, 2).

TABLE I. ENTERPRISE RISK MANAGEMENT LIKELIHOOD

Likelihood Table					
Level	Descriptor	Description	Frequency of Occurrence		
			Strategic	Operational	Routine
1	Rare	May only occur in exceptional circumstances	Less than once every 50 years	Less than once every 10 years	Less than once every 5 years
2	Unlikely	Could occur at some time	At least once in 20 years	At least once in 5 years	At least once in 3 years
3	Possible	Might occur at some time	At least once in 5 years	At least once per year	At least once per year
4	Likely	Will probably occur in most circumstances	At least once per year	At least once per quarter	At least once per month
5	Almost Certain	Expected to occur in most circumstances	More than once per year	At least once per month	At least once per week

TABLE II. ENTERPRISE RISK MANAGEMENT CONSEQUENCES

Consequences Table					
Impact	1 Insignificant	2 Minor	3 Moderate	4 Major	5 Extreme
Safety	No injuries	First aid treatment	Medical treatment, lost time	Medical treatment, extensive injuries	Fatalities
Financial Loss	< $50k or 0.5% of OB	$50k - $250k or 1% of OB	$250k - $3M or 2% of OB	$3m - $10m or 6% of OB	> $10m or > 10% of OB
Asset Loss	Little or no impact on assets	Minor loss or damage to assets	Major damage to assets	Significant loss of assets	Complete loss of assets
Interruption to Services	< ½ day	½ - 1 day	1 day – 1 week	1 week – 1 month	> 1 month
Information Management		Inaccurate data entry	Loss or corruption of database	Failure of backup data	System failure and/or extensive hacking attack
Legislative Compliance		Breach of Regulations	Warning from Regulator	Successful Prosecution	Cessation of Activities
Management Effort	An event, the impact of which can be absorbed through normal activity	An event, the consequences of which can be absorbed but management effort is required to minimise the impact	A significant event which can be managed under normal circumstances	A critical event which with proper management can be endured	A disaster with the potential to lead to the collapse of the University
Reputation and Image	Unsubstantiated, low impact, low profile or no news items	Substantiated, low impact, low news profile	Substantiated, public embarrassment, moderate impact, moderate news profile	Substantiated, public embarrassment, high impact, high news profile, third party actions	Substantiated, public embarrassment, very high multiple impacts, high widespread news profile, third party actions

III. DEFENSE AWARENESS

Part of building a proper structure to mitigate potential and future risks from cyber security attacks involves conducting workshops to educate personnel. Guidelines and training documents provide details on user access privileges. Institutions should maintain an inventory of assets, devices and applications, that a user needs access to, and this is secured with CyberArk, Multi-Factor Authentication is enforced to protect the firm from unauthorized access to corporate assets. Penetration tests are conducted regularly and maintains a robust vulnerability management system to monitor

changes within information systems. Application security policies include written procedures with secure coding standards to ensure secure development of in-house applications.

The following cybersecurity workshops and training are mandatory for executives and employees:

Workshop 1: Agree on which entities to cover and what information is considered nonpublic, as well as the materiality of transactions that relate to audit trail

Workshop 2: Enforce MFA and how to reconstruct an audit trail

Workshop 3: Clarify the certificate of destruction, and the feasibility of the Retention policy

Workshop 4: Train the staff and monitor for threats

Workshop 5: Discuss the feasibility of encryption of nonpublic information and test first line of defense on Microsoft office format documents.

A. Policies and Procedures

A set of 15 must-have policies complements the company's cybersecurity best practices and accompany the strategy to enforce its fulfilment. Policies and Procedures are communicated to all employees. Additionally, where required, appropriate sections are distributed to suppliers and contractors. In doing so, their importance is emphasized. Given that fulfilling them is compulsory, the firm audits compliance, provide continuous oversight, demand accountability, and, where necessary, impose sanctions upon those who violate these rules. The list of policies can be found as an Appendix B.

B. Safety and Physical Security

At any Institutions, employees' safety is a priority. Therefore, counting with the experience of a private security company, specific measures have been taken to ensure the safety of all employees either when working on premises (garage included) or when they travel for work purposes.

On the other hand, understanding that cyber-attacks can sometimes begin with a physical breach -for instance, when an outsider to surreptitiously gather fodder for a social engineering scheme or when an insider (such as a so-called "bad leaver") gains access to a company's network and wreak havoc, without initially using malware or other clandestine technological means- Institutions should take the physical security of facilities into consideration as part of the Cybersecurity strategy. The physical security in the firm's premises including the reception and entry checkpoints; ID scanner and other access records; video; physical logs; and garage records. Safety and physical security measures are audited periodically by a renowned firm to check they are implemented and working as expected, and updated or fixed if necessary.

C. Sytem Development Life Cycle and Change Management

All information systems, including operational systems, systems under development, and systems undergoing modification or upgrade, are in some phase of a system development life cycle. Requirements definition is a critical part of any system development process and begins very early in the life cycle, typically in the initiation phase. Security requirements are a subset of the overall functional and nonfunctional (e.g., quality, assurance) requirements levied on an information system and are incorporated into the system development life cycle simultaneously with the functional and nonfunctional requirements. As recommended by the NIST4, early integration of information security requirements into the system development life cycle is the most cost-effective and efficient method for an organization to ensure that its protection strategy is implemented.

With regard to configuration management and control, it is important to document the proposed or actual changes to the information system and its environment of operation and to subsequently determine the impact of those proposed or actual changes on the overall security state of the system. Information systems and the environments in which those systems operate are typically in a constant state of change (e.g., upgrading hardware, software, or firmware; redefining the missions and business processes of the organization; discovering new threats). Documenting information system changes as part of routine SDLC processes and assessing the potential impact those changes may have on the security state of the system is an essential aspect of continuous monitoring, maintaining the current authorization, and supporting a decision for reauthorization when appropriate.

D. Continuous monitoring

As recommended by the NIST5, a critical aspect of managing risk to information from the operation and use of information systems involves the continuous monitoring of the security controls employed within or inherited by the system. The objective of the continuous monitoring program is to determine if the

set of deployed security controls continue to be effective over time in light of the inevitable changes that occur. Continuous monitoring is a proven technique to address the security impacts on an information system resulting from changes to the hardware, software, firmware, or operational environment. A well- designed and well-managed continuous monitoring program can effectively transform an otherwise static security control assessment and risk determination process into a dynamic process that provides essential, near real-time security status-related information to organizational officials in order to take appropriate risk mitigation actions and make cost-effective, risk-based decisions regarding the operation of the information system. Continuous monitoring programs provide organizations with an effective mechanism to update security plans, security assessment reports, and plans of action and milestones. Using the Template

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper.

E. Monitoring Strategy

The monitoring program is integrated into the organization's system development life cycle processes. A robust continuous monitoring program requires the active involvement of information system owners and common control providers, CIO, CISO, and authorizing officials. The monitoring program allows an organization to: (i) track the security state of an information system on a continuous basis; and (ii) maintain the security authorization for the system over time in highly dynamic environments of operation with changing threats, vulnerabilities, technologies, and missions/business processes. Continuous monitoring of security controls using automated support tools facilitates near real- time risk management and represents a significant change in the way security authorization activities have been employed in the past. The firm uses vulnerability scanning tools, system and network monitoring tools, and other automated support tools that can help to determine the security state of an information system.

F. Monitoring program includes:

- Configuration management and control processes for organizational information systems;
- Security impact analyses on proposed or actual changes to organizational information systems and environments of operation;
- Assessment of selected security controls (including system-specific, hybrid, and common controls) based on the organization-defined continuous monitoring strategy;
- Security status reporting to appropriate organizational officials; and
- Active involvement by authorizing officials in the ongoing management of information
- System-related security risks.

G. Metrics

The results of our cybersecurity strategy are measured through a set of metrics that help us to monitor and control the implementation of the same, better manage our risk and make informed decisions. The list of metrics can be found as an Appendix C.

H. Documentation and Status Reporting

Continuous monitoring results are considered with respect to any necessary updates to the security plan, security assessment report, and plan of action and milestones, since these documents are used to guide future risk management activities. Updated security plans reflect any modifications to security controls based on the risk mitigation activities carried out by information system owners or common control providers. Updated security assessment reports reflect additional assessment activities conducted by assessors to determine security control effectiveness based on modifications to the security plan and deployed controls. The results of monitoring activities are reported to authorizing officials on an ongoing basis in the form of status reports to determine the current security state of the information system, to help manage risk, and to provide essential information for potential reauthorization decisions.

IV. SECTION 0 – TYPES OF ATTACKERS

According to the US Dept. of Homeland Security, "Cybersecurity is NOT implementing a checklist of requirements; rather it is managing cyber risks to an acceptable level. "[6]

Knowing the enemy requires understanding the different threat actors, what their motivations and goals are, how they operate and their sophistication levels, all of which can be used to assess degree of risk. Security experts understand the continuum of threat actors well, based on monitoring and analysis of incidents. A variety of actors with different motivations and objectives are constantly looking for vulnerabilities. These players range from the "inadvertent actor" with no malicious intent to a sophisticated, well-funded and resourceful character that presents a much higher risk of significant impact.

The following table illustrates the types of cyber security actors, with references to historical cybersecurity cases for clarity:

TABLE III. CYBERSECURITY ACTORS. SOURCES: FORTUNE AND MCAFEE

Attacker	Who	Objectives	Targets	Signature	Likelihood	Consequences	Classic Case
State sponsored	China, Iran, Israel, Russia, U.S	Intelligence, state secrets, sabotage	Foreign governments, terrorists, industry	Multi-tiered, precisely orchestrated attacks that breach computer systems	Possible	Major	One-fifth of Iran's nuclear centrifuges crashed after Stuxnet, a worm reportedly developed by U.S. and Israeli intelligence, penetrated computers at an Iranian enrichment facility. Iran allegedly retaliated by disrupting access to the websites of J.P. Morgan (JPM, +1.25%), PNC (PNC, +1.27%), Wells Fargo (WFC, -1.05%), and others.
Hacktivists	Anonymous, AntiSec, LulzSec	Righting perceived wrongs, publicity, protecting Internet freedoms	Bullies, Scientologists, corporations, governments	Leaking sensitive information, public shaming, creepy YouTube videos	Likely	Minor	The websites of PayPal, Visa (V, +0.30%), and MasterCard (MA, -0.05%)were disrupted during Operation Payback, an Anonymous-led effort to punish companies that suspended the accounts of WikiLeaks in 2010. Some $5.6 million was lost by PayPal alone.
Cyber Criminals or black-hat hackers	Nigerian "princes," carders, identity thieves, spammers	Treasure	The gullible, online shoppers, small businesses, data-rich health care and retail companies	Stealing data, looting bank accounts	Possible	Minor	Coreflood, malicious software that records keystrokes and passwords, infected 2.3 million computers in 2009, some in police departments, airports, banks, hospitals, and universities. Affected companies suffered six-figure fraudulent wire transfers.
Insider	Disgruntled employees, contractors, whistleblowers	Score-settling, leaks, public good	Large companies, governments	Document theft	Unlikely	Major	Maroochy Shire, an Australian district along the Sunshine Coast in Queensland, was inundated with millions of gallons of untreated sewage in 2001 when a contractor hacked and took control of 150 sewage-pumping stations. He had been passed over for a job with the district. His dirty work cost Maroochy Shire upwards of $1 million.
Script Kiddies	Bored youth	Thrills, notoriety	Low-hanging fruit such as unprotected websites and e-mail accounts	Defacing or dismantling websites	Likely	Insignificant	An e-mail subject-lined I LOVE YOU duped people -- some of them inside the Pentagon -- in 2001. The virus it contained, which originated in the Philippines, destroyed files and simultaneously replicated itself, seeding in-boxes as it went. The so-called Love Bug caused an estimated $10 billion in digital damage and lost productivity.
Vulnerability Broker	Endgame, Netragard, Vupen	Hacking as legitimate business	Agnostic	Finding so-called zero-day exploits -- ways to hack new software, selling them to governments and other deep-pocketed clients	Rare	Minor	French firm Vupen hacked Google's (GOOG, +0.44%) Chrome browser at a security conference last March. Rather than share its technique with the company (and accept a $60,000 award), Vupen has been selling the exploit to higher-paying customers.
Cyber Terrorists	Terrorists	Spread fear, terror and commit murder	non-believers in their political or religious beliefs	create fear and chaos by disrupting critical infrastructure	Possible	Moderate	Ardit Ferizi was arrested in Malaysia charged in October 2015 with stealing the data belonging to the US service members and passing it to the members of the ISIS with the intent to support them in arranging attacks against Western targets.
Spy hackers	Hackers working for competing corporations	Steal trade secrets	Specific corporations	Leak information that are critical to victim's organization	Possible	Major	Chinese cyber spying of US for military and political reasons.

A. The Cyber Attack Decision Tree

Institutions should implement a Cybersecurity Framework based on NIST7. These are the framework's core functions:

- Identify
- Protect
- Detect
- Respond
- Recover

These core functionalities translate into the following actions:

1) Identify known cybersecurity risks to their infrastructure

2) Develop safeguards to protect the delivery and maintenance of infrastructure services

3) Implement methods to detect the occurrence of a cybersecurity event

4) Develop methods to respond to a detected cybersecurity event

5) Develop plans to recover and restore the companies' capabilities that were impaired as a result of a cybersecurity event

The following attack vectors have been considered and a decision tree based on the framework is provided below:

- Data Loss
- Insider Threat
- Vendor/Partner Compromise
- Compromise of Individual Device
- Phishing
- Network/System Breach
- DDoS Attack
- Ransomware

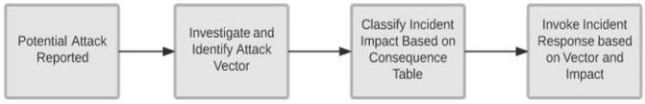


Figure 2. Detect and Identify

When a potential incident is reported, the incident will be investigated to determine if it is valid based on known attack vectors. Once validated, one or more members of the incident response team will collaborate to determine and classify the impact using the Consequence Table. The categories of incidents are insignificant, minor, moderate, major, and extreme. (See Consequence Table)

Each attack vector has the potential to overlap, particularly for data loss or insider threat. One or more of the following decision trees may be put into action depending on the circumstances of the breach.

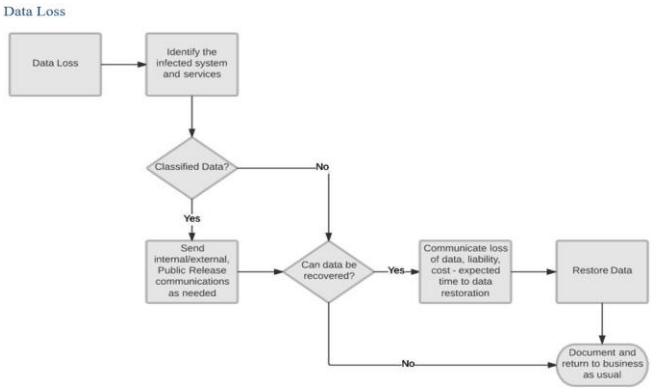


Figure 3. Respond and Recover

An incident that involves loss of data must be immediately analyzed for the loss of classified or sensitive data. If the data contains PII (Personally Identifiable Information), PCI (Payment Card Industry), SOX (Sarbanes Oxley) or other types of data deemed as classified or sensitive, then specific communications will be formulated to the necessary individual(s) and agencies.

The Communications Officer will be responsible for these communications with oversight from the C-Suite, CEO, CISO, CFO and CIO. For any other loss of data, the data recovery, backup and restore will be performed by Information Technology and business will resume as usual.

Figure 4. Insider Threat

If it is determined that any compromise was the result of an insider threat, whether it be a vendor, employee, consultant or former employee, an official investigation will be conducted to determine the goals of the attacker, data loss and entry points on the intrusion. Additionally, the investigation will expand to cover any individuals with close relations to the attacker and identification of additional known conspirators.

Immediately following the identification of an insider threat, the users account will be disabled based on IT guidelines. Furthermore, checks will be performed to identify any unknown accounts and logs will be assessed regularly for other suspicious unauthorized activity.

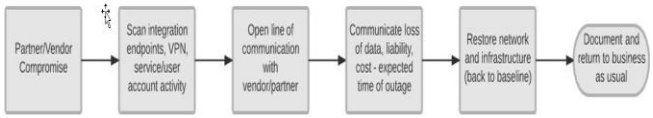


Figure 5. Vendor/Partner Compromise

In the event that a vendor account or endpoint is compromised, a line of communication will be opened with the vendor to assist in identifying the extent and nature of the breach. Data loss and network breach decision trees will be acted upon as well as investigation into any insider threats based on those who have access and knowledge of vendor systems and their inner workings. The goal will be to restore operations with the vendor in a timely manner while gathering the appropriate data to assess the damage and enable additional security protocols to secure the connection in the future.

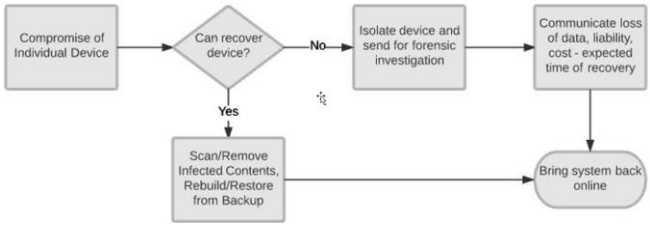


Figure 6. Compromise of individual device

If an individual device is compromised, the Desktop Support team will determine if the device is recoverable through scan and removal of malicious software or through backup and restore. If the device is an unrecoverable state, or the device is known to contain highly sensitive information, the device will be isolated, removed from the network and sent for forensic analysis. The CISO will work with the CIOO to communicate unusual findings.

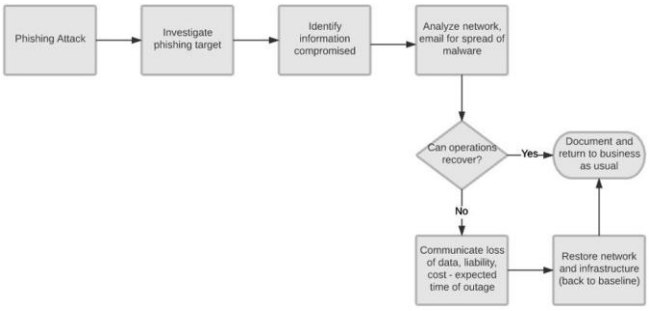


Figure 7. Phishing attack

If there is a malware detection that can be traced back to a phishing campaign, or a user reports a suspicious email or other form of communication that seems like a potential phishing attack, then the decision trees for data loss, system and network recovery will also be enacted.

There will be an investigation into the phishing target with the goal of determining the intention of the attacker and what information they were seeking (See Section 0 on common types of hackers) or may have retrieved. Depending on the extent of the breach, various members of the C-Suite will convene to determine next steps. The Human Resource department will be responsible for investigating the phishing target(s) to determine if any sensitive information was obtained. Further rules for response on data loss or network breach will be followed.

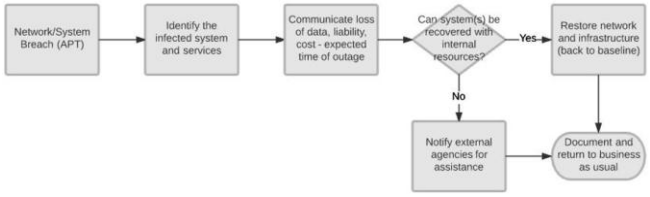


Figure 8. Network systembreach

In the event of an advanced persistent threat (APT), involving a multifaceted breach of network and system resources, it will be determined if systems can be restored with internal resources through collaboration of Information Technology and Information Security. If the breach is beyond internal expertise, external agencies such as the FBI (Federal Bureau of Investigation or DHS (Department of Homeland Security) will be contacted for assistance as needed. All members of the C-Suite, CEO, CISO, CIOO, CFO, as well as HR (Human Resources), will formulate a specific recovery plan and proper communications based on the severity and financial impact to the company by referring to the Consequences Table.

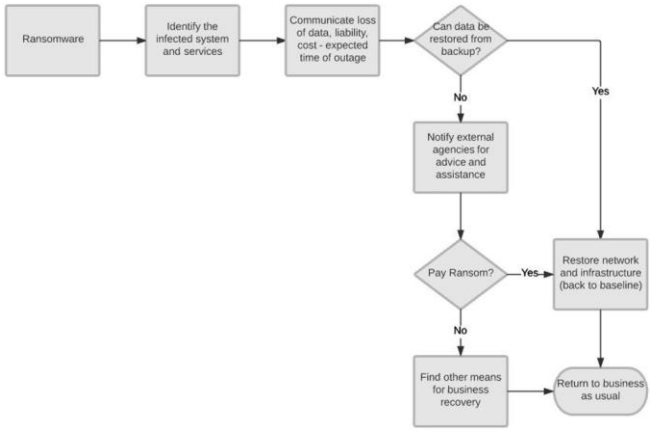


Figure 9. Ransomware

In the unfortunate case of ransomware, where there is potentially unrecoverable data loss through encryption and the data is being held for ransom, the data loss decision tree will also be invoked. If the data is considered classified or sensitive, or poses a risk where the business cannot recover financial loses, than external agencies will be notified for advice and assistance. All members of the C-Suite will be active in assessing the damage of a ransomware attack and determining the proper action.

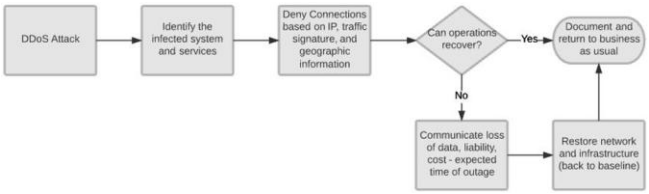


Figure 10. DDOS attack

In the event of a DDoS attack (Distributed Denial of Service), flooding of the network or targeted machines through an overload of requests, the IT Operations team will be responsible for denying traffic and reporting on any potential loss of data and or revenue streams. The CISO will work jointly with the CIOO to communicate the impact of the attack and set expectations for recovery time before returning to business as usual.

B. Protect and Prevent

The CISO will be responsible for cyber security education and overseeing ongoing improvements to cyber defenses. The Incident Response team will review the cyber security playbook quarterly and conduct table top exercises to rehearse incident response procedures. Knowing that attack vectors evolve over time and that attacks become more sophisticated each day, the decision tree will be updated and will adapt to lessons learned.

The cyber security playbook decision tree is meant as a general guideline. Each incident must be accessed and categorized individually and it is the responsibility of the C-Suite to analyze, communicate and react according to the various circumstances of each individual threat.

V. SECTION 2 – C-SUITE RESPONSE

Cybersecurity issues are no longer limited to the Information Technology department. Security breaches threaten every aspect of the organization and pose a significant threat to ongoing business continuity and reputation. These issues extend well beyond the technical environment and reach across the entire business ecosystem.

Cybersecurity solutions must encompass not only technical fixes, but also changes in business processes, controls, and management and employee behavior. Therefore, the Board of Directors understands that being prepared to understand cybersecurity issues, make the key decisions that prevent cyber issues from evolving into full-scale problems, and handle issues from the front-row if presented are the Board's responsibility.

Moreover, the factors that can help "to make the strategy succeed are: identifying information critical to your business; making cybersecurity part of your culture; considering cybersecurity impacts in your decisions; and measuring your progress". (Touhill & Touhill, 2014, Page 124).

As part of the governance model and following the recommendation of the National Association of Corporate Directors (NACD), An Institutions should follow these Five Guiding Principles:

1) Understand and approach cybersecurity as an enterprise-wide risk-management issue, not just an IT issue

2) Understand the legal implications of cyber risks as they relate to their company

3) Have adequate access to cyber security expertise and discussions should be held regularly at board meetings

4) Make sure that management establishes an enterprise-wide risk management framework with adequate staffing and budget

5) Identify which risks to avoid, accept, mitigate, or transfer through insurance.

The following sections detail the response for each C-Suite role:

A. Chief Executive Officer (CEO)

The CEO makes sure that Cybersecurity is incorporated into our strategy as a cornerstone of our business. "Our brand reputation, partnerships, potential investment opportunities, and competitive advantage all rely on the integrity of our information". The following factors have been taken into consideration to make our strategy succeed:

- Identification of the information critical to the business
- Cybersecurity as part of the company's culture
- Cybersecurity impacts considered in all decisions taken
- Measurement of the progress.

There are three initial considerations that the CEO takes into account: first of all, protecting our company against cybersecurity threats goes beyond the pure compliance with standards or regulations. Secondly, we strive to find the balance between cybersecurity and productivity, as. "Cost, performance, and ease of use are key attributes of an efficient and successful cybersecurity program." (Touhill & Touhill, 2014, Page 273). Thirdly, we take into account the risk management lifecycle.

Based on these initial considerations, our cybersecurity strategy distinguishes three **Areas of Focus:**

1) Establishing a governance model for security, including enterprise-wide collaboration,

2) Identifying and protecting critical data and applications, and

3) Developing and implementing an effective response plan.

The details of the Response Plan can be found in Section 1 of this Playbook but the Appendix D includes a comprehensive checklist taken into consideration for the firm's CEO when evaluating cybersecurity and taking major decisions before, during and after an incident.

Regarding the CEO responsibilities and according to the NIST Framework, "the head of agency (or chief executive officer) is the highest-level senior official or executive within an organization with the overall responsibility to provide information security protections commensurate with the risk and magnitude of harm (i.e., impact) to organizational operations and assets, individuals, other organizations, and the nation resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of: (i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

As additional responsibilities, the following are considered:

- Making sure cybersecurity is part of the company's strategy and operational planning, the board discussion and the company's daily routine. This involves transforming the company culture, providing the necessary resources in terms of security systems and security trained personnel, and taking into account lessons learnt from previous incidents (if any) to improve its security posture.
- Creating a Security Committee lead by the CISO and which consists on the members of the C-suite (CEO, CISO, CFO, COO/CIO, Head of Legal/Head of Communication). This committee is in charge of protecting the privacy of corporate and customer data on the network and it from intruders, defining the company's risk posture, engaging 3rd party for hidden vulnerabilities or active compromises, developing and implementing the policies or guidelines required -in compliance with regulations-, and consider cyber insurance for the company and the Directors.
- Overseeing the company's response, especially the communication strategy in close contact with the General Counsel and the Head of Communication.
- Overseeing the damage control especially what is related to approving the investments and personnel needs to strengthen the company's defenses.
- Assisting the law enforcement after an incident -if required- in close collaboration with the General Counsel.
- Repairing the company's reputation with customers, partners, regulators, media, etc. in close collaboration with the Director of Communication.

B. Chief Financial Officer (CFO)

As most firms have the proper C-Suite executives working together in order for a strong collaborative effort to respond to any potential issues, the Chief Financial Officer (CFO) must be aligned for financial data. The CFO works closely already with CEO and CISO to understand the value in the data that could be possibly taken from a cybersecurity breach. From a financial view, the CFO works directly with technology and security to understand the leaks from a breach to manage potential risks. Majority of hacks including ransom cyber-attacks have a dollar value tied to them. The CFO needs to address these type of concerns, plus the costs of remediating the attack with appropriate amount of resources, risk mitigation activities, software upgrades, and patches. The CFO works with General Counsel, Legal, and Director of Communications to analyze the financial impact of the current hack and potential future hacks to understand the deep dive financial matters.

The CFO works directly with the CEO to discuss briefing matters on financials budgets associated with cyber-attacks. Each attack a company encounters needs to be justified to provide the correct amount of costs for man-hours for a patch, and software upgrades to internal systems to build preventive measures within an organization. The CFO is responsible for recommending a budget with C-Suite executives on an annual 3-year rolling forecast to factor in maintenance of upgrades to all internal and external systems that could possibly be faced with any type of cyber threats.

An approved allocated budget from the C-Suite executives allows CTO and CISO to work with external consulting providers to recommend equipment upgrades instead of fulfilling the requirements of hacker if a ransom was requested. It's worth remembering that when a company pays a ransom once, it will flood the gates with additional hackers in the foreseeable future to attack our organization for a quick payment instead of the organization getting cybersecurity expert law enforcement involved. Plus, this type of preventive measure keeps senior management in the loop to keep on investing more in security space of our organization by increasing annual budget to build workshops for firm awareness and risk mitigation.

- Budget: For 2017, the total is $650,000 for consulting and professional services for gap assessments for the year, which will allow senior management to focus on meeting requirements for 2018.
- Budget: For 2018, the total is $14,800,000 with CAPEX and OPEX for GTS/AME accounting for nearly $7,000,000.
- Status/Approach: Feb 2018, key deadlines include setting up a Cyber Security program, with policies and a CISO to manage all three lines of defense. Includes annual penetration testing and annual penetration testing and vulnerability assessments.

C. Chief Information Officer and Chief Operations Officer (CIOO)

Due to our complete reliance on technology to conduct business, the board may decide to combine the roles of CIO and COO into one: the CIOO. The combined role yields pronounced efficiencies/benefits in as far as cybersecurity is concerned, more so during and after attacks.

VI. SCOPE

It is understood that protection against and detection of cyber-attacks is the responsibility of the CISO.

The CIOO partners with the CISO in formulating and executing remediation. The CIOO is equally responsible for:

1) Responding:

a) Apply security patches to vulnerable or affected infrastructure components

b) Isolate/turn off infrastructure components

c) Deploy teams to investigate or remediate issue

2) Recovery:

a) Business recovery (BR) e.g. repair affected application, databases and systems

b) Activate business continuity (BC) plans

c) Activate disaster recovery and service continuity (DR/SCM) plans

Business continuity and recovery components to be addressed during and after a cyber-attack:

3) Adherence to legal, regulatory and governance requirements: refer to the Crisis

Management section of the firm's Governance Policy. The aim is to operate within the governance and regulatory framework even in the event of a crisis.

The objective is to guard against operational havoc by:

a Not violating governance, legal, and regulatory guidelines

b Not opening the door for exploitation of crisis situations by malicious actors

c Maintaining accountability, records and consistency (see figure below)

- **Collaborate with authorities** – SEC, FBI & NSA**.**
- **Address external risks** – partner/supplier relationships and communications
- **Global Context** – political, economic and social changes and events

VII. SYSTEMS CLASSIFICATION

To formulate appropriate responses and communications during a cyber-attack, the CIOO and their delegate would consult with the Applications and Systems Registry which contains, in addition to business and technical information, the appropriate RACI diagram. It should be used as the backdrop against which action is taken (see figure below).

TABLE IV. THE CIOO AND THE APPROPRIATE RACI DIAGRAM

Role	Assess Risk	Manage Risk	Fund Resources	Implement	Assure
Application Owner	I	R, A	R, A	A	A
IT	I	C	I	R	I
Operational Risk	R, A	I	I	I	C
Security	C	C	I	I	R

Responsible: Person or function responsible for executing the activity
Accountable: Person or function that owns the activity, approves work and is held accountable for it
Consulted: Person or function with information relevant to the activity
Informed: Person or function to be informed of progress and results

A. Data Classification

The firm assigns the highest priority in assessing the impact of an attack to the following classes of data:

1) Personally Identifiable Data (PII)

2) Non-Public Material Data (NPMI) such as SEC filing info, board resolutions of clients, etc.

3) Confidential Supervisory Information such communications from the SEC and other regulatory bodies.

Attacks impacting systems housing any of the above three types of data are high risk by nature. The default severity of any such attack is Major until it is downgraded.

B. Cybersecurity Events & Change Management

Since remediation and recovery entail changing components in the ecosystem and infrastructure, the CIO has put in place the following processes:

1) Emergency Change Management – Extreme and Major events justify the activation of these processes where signed pre-approvals are deposited by:

a) Business Application Owners

b) Business Unit Leaders

c) The BoD – subject to final sign-off based on the scope of action where there is:

- A need to communicate externally
- A legal liability
- Financial risk

2) Expedited Change Management – Moderate events warrant a scaled down change process where:

a) Pre-approved Damage Control (limited isolation of components/apps)

b) Fast-track change management - convening skeleton meetings within pre-approved timeframes based on affected apps/components attended by Application Owner and Business Unit representatives.

C. Structure and Delegation

The CIO has two delegates working in tandem and collectively participating in day-to-day business as well as during cybersecurity events:

- VP Operations Management
- VP IT Management

The CIO participation and delegation during cyber events is based on severity as shown below[8.]

TABLE V. THE CIO PARTICIPATION AND DELEGATION DURING CYBER EVENTS BASED ON SEVERITY

Cyber Event Participation Levels

Position	Extreme	Major	Mode rate	Minor	Insignificant
CIO	100%	100%	50%	25%	0%
VP IT	100%	100%	75%	50%	25%
VP Ops	100%	100%	50%	25%	10%

Participation levels are described as follows:

- 100% :
  - Cancel all personal commitments for 72 hours
  - Physically on-site in nearest offices for 72 hours OR if remote, via phone and email with access to appropriate dashboards and/or metrics.
- 75% :
  - Cancel all personal commitments for 48 hours
  - Physically on-site in nearest offices for the first 24 hours OR if remote, via phone and email with access to appropriate dashboards and/or metrics.
- 50% :
  - Keep personal commitments but refrain from alcohol
  - Maintain unfettered access to phone and email communication

- Maintain the ability to join conference calls or video conference meeting as necessary

- 25% :
  - Keep personal commitments and minimize alcohol consumption
  - Maintain unfettered access to phone and email communication o Anticipate periodic status update calls or messages

[8]Please note that a similar model applies to the rest of the members of the C-Suite.

D. Chief Information Security Officer (CISO)

Change is inevitable in every industry. But in finance, the pace of change is driven by regulatory flux, ever changing geopolitical landscape and the constant evolution of technology. Today's financial organizations face an unprecedented array of new challenges in the form of cyber-attacks. According to Cisco, "Playbook is perspective collection of repeatable queries against security event data sources that lead to incident detection and response". Cyber threats are dynamic in nature so it is important for the CISO's to have essential planning and communication skills while protecting shareholder value.

VIII. WHY CYBER SECURITY?

From the CISO perspective, the questions to answer are:

- What am I trying to protect?
- What are the threats?
- How do I detect them?
- How do I respond?

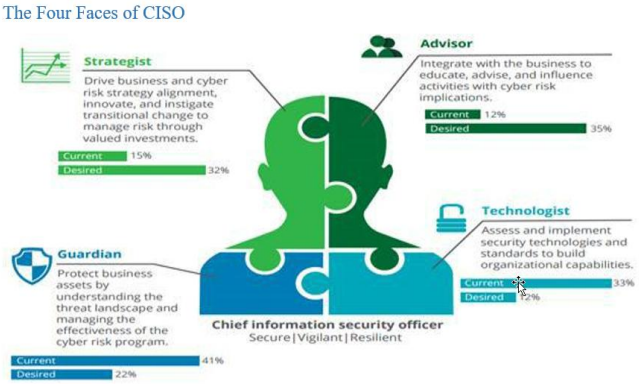


Figure 11. The four faces of CISO

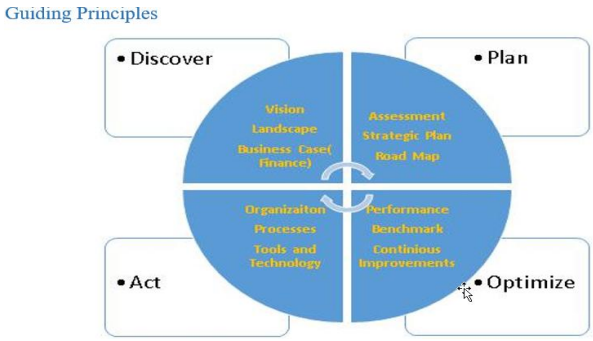


Figure 12. Guiding principles

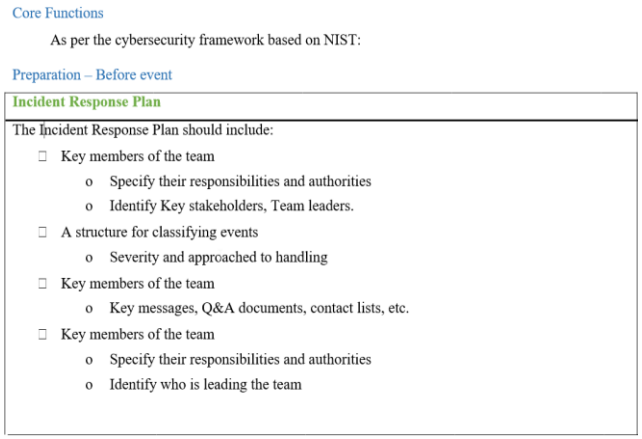


Figure 13. Preparation–Before event

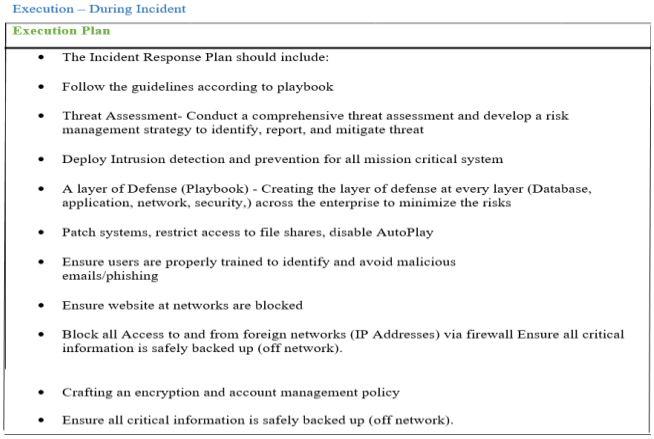


Figure 14. Execution-During Incident

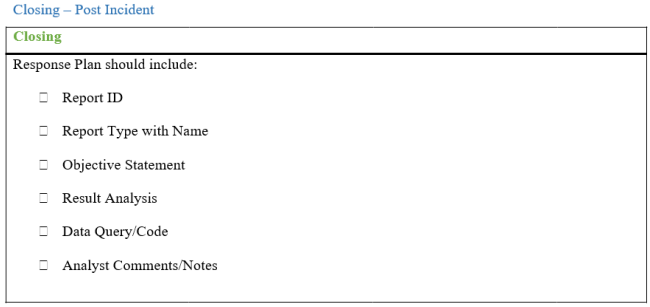
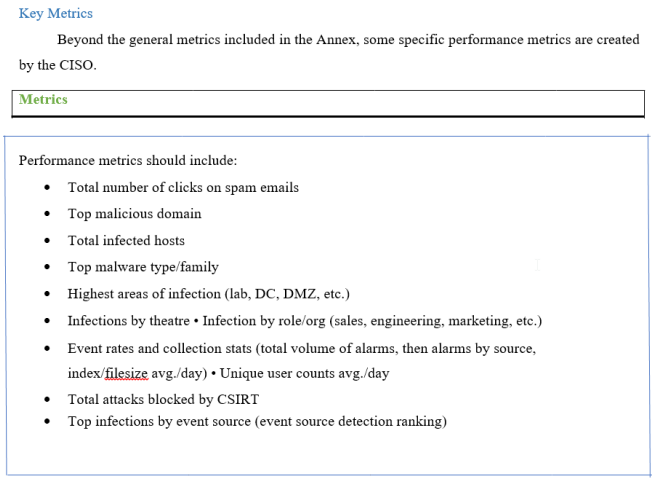


Figure 15. Closing-post incident


Key Metrics

Beyond the general metrics included in the Annex, some specific performance metrics are created by the CISO.

Metrics

Performance metrics should include:

- Total number of clicks on spam emails
- Top malicious domain
- Total infected hosts
- Top malware type/family
- Highest areas of infection (lab, DC, DMZ, etc.)
- Infections by theatre • Infection by role/org (sales, engineering, marketing, etc.)
- Event rates and collection stats (total volume of alarms, then alarms by source, index/filesize avg./day) • Unique user counts avg./day
- Total attacks blocked by CSIRT
- Top infections by event source (event source detection ranking)

Figure 16. Key Metrics

IX. LEGAL COUNSEL (AKA GENERAL COUNSEL)

The Legal Counsel side of the issue is critical to the attack, applying to the regulations of the state or country will prevent further damage in the form of lawsuits or penalties. Rules such as the GDPR needs to be adhered to because if found that after an attack not all proper precautions were followed according to the guidelines, a hacker will be the least of our worries. While legal is necessary for incident response, following the proper protocols ensures an attack has minimal damage.

A. Key concerns for General Counsel heavily revolve around compliance to meet Federal Mandates

It is a sole responsibility for C-Suite Executives to be aware of all information security regulations that apply to the company, such as Health Insurance Portability and Accountability Act (HIPAA), 1999 Gramm-Leach-Bliley Act, and the Federal Information Security Management Act (FISMA) as part of the 2002 Homeland Security Act, General Data Protection Regulation (GDPR), and Payment Card Industry Data Security Standard (PCI DSS). General Counsel needs to work with both CISO and CIO to ensure information system security practices follow proper guidelines. Moving forward we need to be up to date on National Institute on Standards and Technology on best practices of cyber security infrastructure and policies.

Next aspect of General Counsel is to ensure that audits follow proper methodology for Federal Review and are set in place in order to produce efficient controls. Keeping semi-annual audits of internal information security infrastructure, where a draft is written up to help conclude how the system can be improved. With all of the Third-Party vendors working with our organization we need to ensure audits are conducted based on information security policies and systems will not be a liability to the company. General Counsel needs to adhere to best practices in risk management so as to have minimal or no damage in an attack.

The General Counsel moves in the direction to ensure that proper law enforcement barriers are set up in our preventive measures and resolution plan. We have drafted a created list based on scenarios on how much damage and type of damage expectations to occur before involving the federal authorities. Internally, within our organization, we have established connections with security clearance authorities as well to understand the scope of the investigation to address how it will affect the firm's information and business processes.

General Counsel has developed a proper Data Retention Policy for internal employees and external clients to keep data secured then protected. We need to understand the policies of data retention of how to properly manage and maintain data as evidence in case of a customer request for information (RFI). Then a major focus is on ensuring the integrity of the data is preserved as well as having documented the chain of custody which begins in the collection phase.

General Counsel have created the proper documentation to executive opinions that could possibly affect Attorney-Client privilege. The knowledge of the incident response fall under normal operations and which are protected under attorney client privilege. Counsel should be involved in all communication whether it be phone, email, etc. between company and the cyber security consultants brought in for the attack. Direct contact with General Counsel is required immediately after an attack as the worst part of the attack is right after it has taken place because of speculation on incomplete information, damaging communication is likely to occur.

1) Compliance

As we are in a growing age of cyber security breaches and constant hacks from outside parties of each organization, the laws of data security and provisioning have been increasing. The US Regulators have forced organizations with client and customer data to take increase precautionary methods to ensure governance. Some of these types of new regulations include Department of Financial Services (DFS) Cyber Law, GDPR, Multi-Factor Authentication, and Third-Party Security Program.

The DFS Cyber Law remediation plan is heavily focused on proper governance requirements to meet Federal Requirements by FINRA. As the need for proper preventive methods, C-Suite Executives turn to Legal Counsel to build property strategies to implement a strong cyber security infrastructure that resembles all divisions of the company from Front to Back office. This includes a program to design a risk based approach with policies to address key elements reviewed by the General Counsel and CISO to oversee the program.

The General Counsel will need to translate Federal Requirements to build a variety of tools with alignment from all areas of the organization. These types of technical implementations include Multi-Factor Authentication to network access, encryption to protect information, and breach notification to notify the DFS within 72 hours of a cyber-attack. With the new mandates being consistently brought up in the media, it is aggressive timeline to implement these requirements based on the increase amount of threats within cyber-attacks. Information Technology stakeholders globally such as ITEC and GTS will help with the execution and regulatory requirements such as GDPR outline exactly what is needed to be followed for US regulations.

2) Guidelines for Compliance

Purpose: Law requires banks regulated by DFS to establish and Maintain Cyber Security Program

- **Section 1**: Compliance by August 28, 2017 such as CS program, policies, and CISO
- **Section 2**: Compliance by March 1, 2018 such as MFA, Training and Risk Assessment
- **Section 3**: Compliance by September 2, 2018 such as Audit Trail, Data Encryption and Monitoring
- **Section 4:** Compliance by March 1, 2019 such as Third-Party Security Program

B. Director of Internal and External Communication

The main responsibility of the Director of Internal and External Communication in a cybersecurity breach is to keep the public aware of any risk mitigation issues and a strong response to the media that we as C-Suite level employees are ensuring best practices to safely protect the data of our customers. In this day and age, it is very crucial to develop relationships outside the organization with correct media outlets to release significant details while gaining the trust of our shareholders. These types of breaches have in the past caused many issues by not focusing efforts on communication and keeping shareholders and stakeholders in the loop.

1) Internal Communication

Internal communications address two groups that will include the employees as well as any business partners. Effective internal communications will mitigate the need of panic by individuals and organizations who are working in the company or with the company. If employees or business partners panic and make consequential decisions based on incomplete information they could cause much more harm than the attack itself. An effective communication plan will allow for smooth flow of information at the time of crisis so attention can be given to the more pressing issue of how to stop the attack and not with its secondary effects.

Managing the internal communication between employees and C-Suite is a fundamental need quickly as a response. This keeps employees in the loop and aware not to communicate outside of the organization that could reflect negatively within the media. Right away as soon as the attack occurs and management is notified, all employees will receive an email from Human Resources. This information will report that a breach has occurred and further information will be made available as soon as possible. Also, all internal emails by non-members of the internal team investigating the incident should cease because speculation could cause unnecessary panic. There will be a request to not use social media at this time and listing the consequences of misinformation can cause. All Information Technology senior management will receive a separate protocol which depending on the specifics of the attack will notify how their department will be responding to the attack. The CISO here will be the main supervisor in charge of all necessary changes that need to be made to any information systems.

Other banks and broker-dealers our firm does business with should be notified in a proper response method in order to protect business with our partners. If the company has any legal obligations to inform of an attack in a specified amount of time as is the case with the GDPR regulations on breach notification, let the entity know of the attack, whether it be for compliance, insurance, or CIRT. Let any business partners know how any vulnerabilities to their information, so they can begin any incident response plans to help keep their business from being affected by the attack.

2) External Communication

External Communications will focus on stakeholders of the company as well as the media. External communications will be less specific and will be to keep the public image of the company as one that in top of the attack and give assurance to stakeholders and customers alike. A great example of bad external communications is the SONY hack, where SONY's reputation was tarnished for not standing up to the hackers.

Based on external communications a major area of concentration needs to be on top of the stakeholders and shareholders in the organization to get the latest up to date information. This type of direct involvement by C-Suite executives makes shareholders feel part of the organization with engagement notifications. The focus on these type of communications is based on specifics of the cyber-attack, the plan created to ensure that the company does not allow further information or data to be viewed in public mindset. The communication externally will be able to then come up with a strategic plan to discuss increase in security controls, password resets, identification requirements, and preventive measures for a patch. The communication that will be shared with the public will be drafted by the C-Suite to explain all of the above with additional answers to questions faced by media scrutiny.

Managing Public Relations is going to be key in our cyber breach playbook. Depending on the scope of the attack, a strong Public Relations response and resource will need to be positioned here as majority of the C-Suite will be completely consumed in responding to the attack. The first response to the media will be crucial in order to have control of any negative news that could hurt our organization. The company will make it a top priority to have the appropriate response in order to set up proper damage control and manage expectations. The public relations team will have to set up proper contacts within each media organization ahead of time to reveal minimal details of the attack and assure the public of the risk mitigation activities being performed by senior management.

3) Communications to regulators

The firm has decided to adopt a doctrine of transparency in reporting cybersecurity attacks, despite the fact that the practice is optional. The reporting, however, is qualified in that it should apply only to Extreme and Major events. The rationale is that the company needs to guard against long-term reputational loss/damage, despite the short-term risks of stock price fluctuation. In the event of Extreme and Major attacks, the executive board will approve communications based on form 8-k using Fish & Richardson Disclosure Decision Tree depicted in figure below:

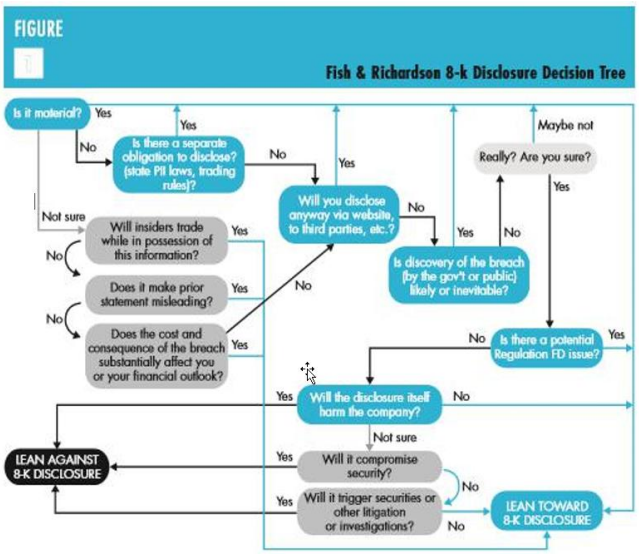


Figure 17. Appendix A. Organization Chart

TABLE VI. APPENDIX B. CYBERSECURITY POLICIES

Retrieved from (Touhill & Touhill, 2014, Page 197)

1. Acceptable Use Policy	6. Employee Internet Use Monitoring and Filtering Policy	11. Remote Access Policy
2. Computer Ethics Policy	7. Technology Disposal Policy	12. Mobile Device Policy
3. Password Protection Policy	8. Physical Security Policy	13. Software Policy
4. Clean Desk Policy	9. Electronic Mail Policy	14. Access Control Policy
5. Use of the Internet Policy	10. Removable Media Policy	15. Network Management Policy

TABLE VII. APPENDIX C. CYBER SECURITY METRICS

Question	Metric Category	Metric
How Vulnerable Are We	**1.0**	**Number of Threats Detected**
	1.0.1	How many times are we being "pinged" and "probed"?
	1.0.2	How much spam is filtered?
	1.0.3	How many phishing messages are we receiving?
	1.0.4	Who is targeting us?
	1.1	**Number of Known Vulnerabilities**
	1.1.1	System vulnerabilities
	1.1.1.1	Number of vulnerabilities discovered
	1.1.1.2	Percentage of vulnerabilities mitigated in prescribed time frames
	1.1.1.3	Number of residual vulnerabilities
	1.1.2	Other Vulnerabilities
	1.1.2.1	Percentage of systems and devices beyond projected life span
	1.1.2.2	Percentage of software beyond projected life span
	1.2	**How Many Cyber security Incidents Have We Detected?**
	1.2.1	Number of cybersecurity incidents detected
	1.2.2	Number of detected cybersecurity incidents by category
	1.2.3	Cost per incident
	1.2.4	Who is responsible for cyber security incidents
How Effective Are Our Systems and Processes?	**2.0**	**Network Performance Measures**
	2.0.1	Network Performance Measurement
	2.0.2	How does network performance compare to previous measurements?
	2.0.3	Percentage of devices with current security software
	2.1	**Change Management**
	2.1.1	Number of unauthorized changes, Unauthorized changes to your systems are not good
	2.1.2	Percentage of maintenance successfully accomplished within schedule and budget
	2.2	**Software configuration management**
	2.2.1	Percentage of software current with all known patches. This is a critical cybersecurity measure. It makes sense to patch your soft
	2.2.2	Number of unauthorized software and media detected on network and devices
	2.3	**Physical Security**
	2.3.1	Number of physical security incidents allowing unauthorized access into facilities
	2.3.2	Number of violations of clean desk policy
	2.4	**Acquisition**
	2.4.1	Percentage of System and service contracts that include security Requirements and/or Specifications
Do we have the right people, are they properly trained, and are they following proper procedures?	**3.0**	**Percentage of employees who have current Cybersecurity training**
	3.1	**Percent of technical staff with current certifications**
	3.2	**Number of Users with system administrator privileges**
	3.3	**Number of security violations during reporting period**
	3.4	**Percentage of security incidents/violations reported within required timelines**
Am I Spending the Right Amount on Seurity?	**4.0**	**Cyber security Costs**
	4.0.1	Percentage of the IT budget devoted to cybersecurity
	4.0.2	Percentage of the organization budget devoted to cybersecurity
	4.0.3	Execution of current budget
	4.1	**Value of Information**
	4.2	**Consequences of Information loss, Tampering, or Destruction**
	4.2.1	Cost to replace
	4.2.2	Estimated costs associated with loss, tampering, or destruction of information
	4.2.3	Estimated costs associated with regulatory fines for failing compliance
	4.3	**Cybersecurity Risk Exposure**
	4.3.1	Cybersecurity risk

TABLE VIII. APPENDIX D. CHECKLIST FOR CEO(EXECUTIVES IN GENERAL)

Appendix D. Checklist for CEO (Executives in general)

Retrieved from (Vantage Point, 2016)

Before an Incident

1 - Stay current on the latest threads and cyber security best practices	4 - Research, design, and deploy security technology. Consider access control, data security, training, processes, and procedures	7 - Ensure the response plan covers communications, analysis, mitigation, and other critical tasks	10 - Discuss with counsel whether cybersecurity risk factors in the company should be disclosed (i.e. SEC 10-K filings) in public
2 - Designate a board committee tasked with cyber security responsibilities. Establish links between board and C-level executives, specially CIO and CISO	5 - Develop and deploy the appropriate systems to identify a cyber security event as soon as possible	8 - Run practice drills to test the plan and revise it as needed	11 - Obtain liability insurance specifically covering cyber security risk for directors and officers as well as for the corporation
3 - Identify the firm's security posture and the risks to the company. Assess the company's systems, assets, data, and capabilities. And identify risks unique to your industry	6 - Create an incident response plan that lays out who reports to whom. Build in contingencies in case some people are unavailable at the time of an incident	9 - Establish a recovery plan to restore any capabilities or services impaired by a breach and to protect the company from further attacks	12 - To limit the company's liability in certain kinds of attacks, consider cyber security vendors certified by U.S. Department of Homeland Security's SAFETY ("Support Anti-Terrorism By Fostering Effective Technologies") Act

TABLE IX. ONE EVENT FOLLOWED BY ANOTHER

During an Incident

1 - Oversee an incident response. Serve as a conduit between incident responders within the company and external stakeholders including customers, partners, and regulators	2 - Understand that news of the incident usually comes to the company from outsiders, such as law enforcement or partner companies. Keeping the event under wraps is no longer very likely	3 - Work closely with your legal counsel and public relations team to advise C-level executives about how to disclose incident details, especially to news media. Don't disclose facts until they've been verified	4 - Stay in touch with your response team to assist as needed during response and through remediation

After an Incident

1 - After a breach has been repaired, intruders ejected, and systems restored, assist in damage control to fix the company's infrastructure and reputation	2 - Review incident response to assess how it went. Identify weaknesses in equipment, systems, and procedures to determine where to make improvements	3 - With guidance from your legal counsel, determine how to make customers whole if their data was exposed or stolen	4 - Consider offering free credit monitoring, issuing new account numbers, and so on. Identify the "churn rate". Counsel can advise as to any consumer remedies required by law

REFERENCES

[1] Morgan, S. (2015, November 24). IBM's CEO On Hackers: 'Cyber Crime Is The Greatest Threat To Every Company In The World'. Retrieved August 05, 2017, from https://www.forbes.com/sites/stevemorgan/2015/11/24/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/#75f85d3973f0

[2] Global Cost of Cybercrime Predicted to Hit $6 Trillion Annually By 2021, Study Says. (2016, August 16). Retrieved August 05, 2017, from http://www.darkreading.com/attacks-breaches/global-cost-of-cybercrime-predicted-to-hit-$6-trillion-annually-by-2021-study-says/d/d-id/1326742

[3] Cybersecurity Questions for CEOs. (n.d.). Retrieved August 5, 2017, from https://www.us-cert.gov/sites/default/files/publications/DHS-Cybersecurity-Questions-for-CEOs.pdf

[4] Fry, E. (2014, June 12). The 6 worst kinds of computer hackers. Retrieved August 05, 2017, from http://fortune.com/2013/02/26/the-6-worst-kinds-of-computer-hackers/

[5] M. (2016, October 24). 7 Types of Hacker Motivations. Retrieved August 05, 2017, from https://securingtomorrow.mcafee.com/consumer/family-safety/7-types-of-hacker-motivations/

[6] Enterprise Risk Management Consequence and Likelihood Tables. (n.d.). Retrieved August 6, 2017, from https://ppl.app.uq.edu.au/sites/default/files/Risk%20Consequence%20and%20Likelihood %20Table%20-%20Form.pdf

[7] Touhill, Gregory J., and C. Joseph Touhill. Cybersecurity for Executives, Wiley, 2014. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/columbia/detail.action?docID=1707094.

[8] Wheeler, E. (2011), Security Risk Management, Chapter 8, Risk Evaluation and Mitigation Strategies, Elsevier Inc.

[9] Institute, F. (n.d.). FAIR, an international standard by the Open Group. Retrieved August 08, 2017, from http://www.fairinstitute.org/an-international-standard

[10] Deinert, A. (2016), "Cybersecurity Breach Playbook: What Every IT Administrator Needs to Know", Vantage Point Solutions, Mitchell, SD

[11] Framework for Improving Critical Infrastructure Cybersecurity. (n.d.). Retrieved August 8, 2017, from

[12] https://www.bing.com/cr?IG=46B942FD8FD04ED7A2EF4DE7E061BAE0&CID=18B3474BBA4361240BCE4D93BB45607D&rd=1&h=qHbOGImxzOpDg5E54Eh7p9I1gen0wVX Vy1g-wVCQk6w&v=1&r=https%3a%2f%2fwww.nist.gov%2fdocument-3766&p=DevEx,5063.1

[13] Cichonski, P. R., Millar, T., Grance, T., & Scarfone, K. (2017, February 19). Computer Security Incident Handling Guide. Retrieved August 08, 2017, from https://www.nist.gov/publications/computer-security-incident-handling-guide

[14] Cichonski, P. R., Millar, T., Grance, T., & Scarfone, K. (2017, February 19). Computer Security Incident Handling Guide. Retrieved August 08, 2017, from https://www.nist.gov/publications/computer-security-incident-handling-guide

[15] NIST. (2014, February 12) Retrieved from https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

[16] Scholtz, T., McMillan, R. (2017, January 26). Institute Cybersecurity and Risk Governance Practices to Improve Information Security. Gartner.

[17] Kark, K., Francois, M., Aguas, T. (2016, July 25). The new CISO: Leading the strategic security organization. (n.d.). Retrieved August 09, 2017, from https://dupress.deloitte.com/dup-us-en/deloitte-review/issue-19/ciso-next-generation-strategic-security-organization.html

[18] Fry, E. (2014, June 12). The 6 worst kinds of computer hackers. Retrieved August 09, 2017, from http://fortune.com/2013/02/26/the-6-worst-kinds-of-computer-hackers/

[19] M. (2016, October 24). 7 Types of Hacker Motivations. Retrieved August 09, 2017, from https://securingtomorrow.mcafee.com/consumer/family-safety/7-types-of-hacker-motivations/

[20] https://www.us-cert.gov/sites/default/files/publications/DHS-Cybersecurity-Questions-for-CEOs.pdf

[21] https://www.forbes.com/sites/stevemorgan/2015/11/24/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/#bfb909373f07

[22] http://www.darkreading.com/attacks-breaches/global-cost-of-cybercrime-predicted-to-hit-$6-trillion-annually-by-2021-study-says/d/d-id/1326742

[23] G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references)*

[24] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[25] I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[26] K. Elissa, “Title of paper if known,” unpublished.

[27] R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[28] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[29] M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.

[30] Electronic Publication: Digital Object Identifiers (DOIs):

Article in a journal:

[31] D. Kornack and P. Rakic, “Cell Proliferation without Neurogenesis in Adult Primate Neocortex,” Science, vol. 294, Dec. 2001, pp. 2127-2130, doi:10.1126/science.1065467.

Article in a conference proceedings:

[32] H. Goto, Y. Hasegawa, and M. Tanaka, “Efficient Scheduling Focusing on the Duality of MPL Representatives,” Proc. IEEE Symp. Computational Intelligence in Scheduling (SCIS 07), IEEE Press, Dec. 2007, pp. 57-64, doi:10.1109/SCIS.2007.357670.