HARVARD
Office of the Vice Provost for Advances in Learning

CYBERSECURITY:
MANAGING RISK IN THE INFORMATION AGE

Cyber risk mitigation strategy for newspapers
A case study
By Carmel Tse

Course convener:
Eric Rosenbach
Harvard Kennedy School

HARVARD
Office of the Vice Provost for Advances in Learning

HarvardX

Learning outcome:

Develop a cyber risk mitigation strategy specific to your organization.

Plagiarism declaration:
1. I know that plagiarism is wrong. Plagiarism is to use another's work and pretend that it is one's own. **2. This assignment is my own work.** **3. I have not allowed, and will not allow, anyone to copy my work with the intention of passing it off as his or her own work.** **4. I acknowledge that copying someone else's assignment (or part of it) is wrong, and declare that my assignments are my own work.**

This module focused on the importance of risk mitigation and the value companies can derive from implementing a risk mitigation strategy to improve organizational resilience and manage risks effectively. This assignment requires you to complete a cyber risk mitigation strategy for your organization.

As the notes made clear, a risk mitigation strategy helps an organization prioritize its risks so it can allocate resources efficiently. This final submission is an opportunity for you to reflect and condense all the knowledge you have gained over the duration of the course by incorporating feedback from your previous ongoing project submissions into a consolidated cyber risk mitigation strategy.

Note:

All ongoing project submissions throughout the course need to focus on the **same** organization. This case study uses a newspaper group's operation in the New York area.

To avoid disclosing any confidential information in this assignment, the name of the organization and brands used are removed. The assignment is drawn on real-world experience but sensitive details or data have been removed or altered.

Introduction

The media, be it print or digital, are subject to cyber vulnerabilities on multiple fronts, more so than most other sectors. Although the media industry was not in the top six, we in the fourth estate face risks that no others would – we are seen as highly opinionated and considered to have influences. As long as we are perceived to have influences, we are threatened.

The risks

Editorial stance on geo-political issues. The media's job is to report news, especially bad news. When the subjects disagree, they interrupt.

Political coverage. Even the POTUS doesn't like some of us, let alone other politicians.

Organized crime coverage. Some of our colleagues lost their lives for doing their job.

Impact on the financial markets. Our stories can send shockwaves to the market.

Disagreement with what we publish. In the old days, they sent letters to the editor. Since 2001, they sent anthrax.

Vision

Our vision is by Q1 2020, our company will have implemented a secure and resilient cyber environment to secure our assets, protect our investors, train our workers, safeguard the privacy of our customers, and use new innovation and technology to grow our business in the new information decade.

If we look back 30 years and plan our next cybersecurity decade based past key developments, we might be able to plot – not imagine – the cyber path we may have to go through in the next decade.

1990s

- Arpanet becomes the internet
- SSL encryption for transactions implemented
- 2G wireless phone technology introduced

2000s

- Advanced Encryption Standard (AES) for classified information
- ILOVEYOU worm spreads
- iPhone, Android, 3G introduced
- Aurora with Chinese footprints attacks Google and 33 other businesses

2010s

- Yahoo, Target, Sony, Anthem, Ukraine power grid breached

- WannaCry ransomware attacks
- U.S. banks hit
- 4G introduced, 5G hatching
- U.S. curbs ZTE and Huawei activities

Tel: +1 519-673-7333 | **Email:** ctse@qint.com

Strategic goals and objectives

Bad actors will continue to cut through our digital fences, intrude into our properties, interrupt our business, steal customer data and may alter our digital assets. Through four broad strategic goals, our plan is to move in parallel in the following measures:

> **Prepare.** This is a top-led initiative and directions will have to start at the leadership level with support of the board of directors. Funding is a top priority. The initiative will filter down to all in the organization.
>
> **Secure.** This will focus on fortifying our perimeters, discouraging intrusions, encrypting our data and strengthening security for passages through our gateways.
>
> **Defend.** We have to be vigilant and be prepared to be fend off and chase out any invasions through preemptive strikes, removing any sleeping malware before they start attacks. Our arsenal shall include latest detection software, scalable cloud storage and eradication tools. Wargames will be used to prepare our strike teams and all staff will be trained to be cybersecurity aware.
>
> **Forward thinking.** Technology does not freeze on January 1, 2020. We will have to adjust and revise our cybersecurity initiatives from time to time.

To achieve our strategic goals, initiatives must be based on risk mitigation and we need to prioritize on the following objectives:

Prepare.

- Initiatives are to be spearheaded by the leadership. The CISO will direct the cybersecurity effort and a cybersecurity manager will project manage the tasks.
- Initiatives must have the full support of the governing body and funding be allocated.
- A strike force will be set up with members accredited with proper certification. All other staff will be furnished with cybersecurity awareness training.
- Initiatives will be cross departmental with minimal barriers.

Secure.

- Firewall to be examined and updated with latest software and hardware defenses.
- Outside of the firewall, websites to be migrated to scalable cloud storage.
- Remote access to be implemented with more secured two-factor authentication.
- On-site authentication to be upgraded to use secured password requirements.
- Encryption of different data types to be reviewed and implemented.

Defend.

- The organization has to have the capability to detect and eradicate threats before they will exert harm on the systems, in that we need to rely on artificial intelligence and machine learning.
- Defensive tactics and weapons are to be one-step ahead of bad actors.
- Collaborations are to be established with industry peers and enforcement agencies.

Forward thinking.

• As part of the procurement process, we will require our suppliers to constantly review their products and services to take into consideration arising threats.

• Blended into the future will be the maturing of the fifth-generation wireless technology. As a media, 5G will govern how will distribute our products and further interact with our customers through the internet of things. We aim to be 5G ready as soon as it's available.

Metrics

The No. 1 metrics to measure achievement is the buy-in by the board of directors. This is to be followed by funding allocation and appointment of the cybersecurity leadership. A general cannot win the war without soldiers and cybersecurity staff has to be in full compliment.

The progress of the cybersecurity initiatives will be tracked and calculated using a Gantt chart. In this type of projects, a cross-departmental waterfall project management schema may be more effective than an agile model. The cybersecurity project manager is the steward of the Gantt. Training and certification, as examples, are best tracked with targeted start and finish dates. Other tasks that can be tracked by the Gantt chart includes 2FA, password policies and encryption sub-projects.

To really test the effectiveness of the initiatives, results of the wargames are good indicators of how ready we are. The wargames should be umpired by an outside judge.

Threat actors and methods of attack

Nation states. Journalists are highly opinionated and our views are often dislike by nations states being criticized. In 2017, 65 journalists lost their lives related to their assignments, and in 2018, 45 had died with the most notable being Jamal Khashoggi of the Washington Post who disappeared at the Saudi embassy in Istanbul. We are monitored.

Hostile nation states often have the resources and technologies to interrupt our operations. Many DDoS attacks have Chinese and Russian footprints. They may even exert influences using us during election campaigns.

PR agencies. Public relations firms are often hired to conduct press conferences and distribute press releases. It is common USB storage devices are given out with press releases

or at press events. Journalist covering conventions in foreign countries are often offered sim cards or even whole mobile phones. We have been warned of potential malware or worms.

Contending entities, including foreign governments, businesses, NGOs, celebrities, politicians, often use PR agencies to spread their messages – good or bad.

Even if we just used the wi-fi service provided, our laptops, tablets and phones might be infested. And if those devices are connected again inside our network, the whole organization can be affected.

Criminals. Newspapers own a large amount of customer data, including payment card information, reading preferences, home addresses and contact information.

If the privacy of our customers are breached, we will be in serious financial liabilities.

Insiders. The most senior writers at newspapers are usually not very computer savvy. They are excellent wordsmiths but when it comes to technology, most of them are at a lost. They are highly vulnerable to phishing schemes. At the other extreme, are the interns. Each year newspapers take in interns to fill in for summer vacations. They are computer whiz and curious, but often given full network access.

Our correspondents. Many of our reporters, columnists and contributors are based in foreign countries. They file their stories using their laptops from press centers, hotels or sometimes even internet cafes. Even if they use their cellular data to file, the host country's phone networked is heavily monitored or censored. There is always a risk that data transmitted may have been hacked or have viruses attached.

Newsfeeds. We take in on average more than 20,000 stories a day at each newspaper from wire agencies like AP and Reuters. If someone wants us to publish a fake story for just 15 minutes, they can disguise as AP or Reuters which will give the story a lot of credibility, it could potentially send shockwaves to the financial markets. A long or short position on certain securities may be profited.

Innocent readers. Our readers usually like us otherwise they wouldn't be subscribing. Because some of them may have access to certain restricted areas on our network because of their subscriber status, their accounts may have been hijacked or piggy-backed, carrying harmful malwares that may eventually make their lateral moves within our secured networks.

Contractors. From the cafeteria's vending machines to our content management systems, our tools are almost always serviced by outside contractors. Some of them may come on site to work while others may connect remotely to render their services. These are the people we trust but there is no guarantee that they have cybersecurity policies as stringent as ours.

Business critical assets

The media is usually the first to expose other's cybersecurity flaws, mostly at governments or large corporations, but when it comes to our own information, we are quite vulnerable.

Editorial systems

Editorial systems are unique compared to systems of other industries – we attract opponents who disagree with us. The players can be nation states, big PR firms, interest groups and even disgruntled individuals. The attackers are sometimes well resourced. Some attackers also aim to profit by impacting the financial markets.

The media's routine is to collect information, verify and reorganize them, and distribute them for consumption. Almost all editorial systems involve integrated technologies.

Gateways. The information comes from various sources: reporters, press releases, readers' input and newswire services. The information eventually ends up in file servers but they all arrive through gateway systems. Some gateways are accessible to the public but most are restricted to authorized users. Examples of gateways include: VPN, remote access, internet portals, emails, USB storage and wire service feeds. The numbers are vast and as an example, a medium-sized paper receive more than 20,000 stories a day.

Risk: Gateway attract malwares and tailgaters.

Content management systems. Reporters create stories in the CMS. Once the information enters the network, it becomes an asset and is stored in CMS. The assets typically are text, pictures, graphics, videos and audios. They are indexed and metadata is attached to each asset for identification. When assets are checked out for editing and checked in for storage, audit trails are established. The CMS also composes print and web pages. CMS are supposed to be off limit to the public.

Risk: Data is the media's **most essential asset**. It is time sensitive as old news is worth nothing. In the event of a destruction, recovered data may deem useless if it passes its shelf life.

Distribution systems. For traditional products, this includes printing, circulation and broadcast. The systems are restricted and mostly protected.

With digital, information is available instantly once released from the CMS. Stories and videos populate the media's web site which are fully accessible to the public. The web sites, sitting outside of the firewall, are the most likely targets of attacks through hacking and DDoS.

Risk: When distribution shuts down, products cannot reach the customers. Most news organizations use social media as backups.

Non-editorial systems

Servers and network. File servers are data warehouses and depositories for the different systems. Risk exposures are lessened with the emergence of cloud storage.

The servers and editorial systems are integrated together through local and wide area networks. The gateways, CMS and printing systems are protected behind firewalls with limited ports open to the outside world. Within the organization, user devices are protected by network segments based on job functions.

Business and advertising systems. Our business database incorporates a lot of our customers' private and financial information. For individual customers, these may include subscription, classified ads, personal announcements, intimate relations and buy-and-sell information. For corporate customers, these may include information on unreleased merchandises, including product description, new features, pricing structures and competitive data.

Cybersecurity governance

1. Governance

Cybersecurity guardianship at most media is tiered between corporate and local management. Newspapers, in particular, have gone through large ownership changes in the last decade through mergers and takeovers. Corporate management reports to a board of directors who in turn reports to the shareholders. Local management reports to their corporate counterparts.

Most new owners tend to keep the identities of the local masthead as they want to assure readers their newspapers would remain the same after ownership changes. Plus, many new owners have little knowledge about the biggest asset of their acquisition – the content management system (CMS).

While chains should have standards covering issues such as enterprise information security policy (EISP), email and domain controls, the operation of the newspapers and the control of the CMS remain in the hands of the local operating committee. OCs typically include the publisher, editor-in-chief, chief financial officer, advertising director, marketing director, operations director and IT director. This is the local C-suite team.

The team also has autonomy in choosing equipment and suppliers as contractor qualities vary greatly by regions. Newspapers bought or merged often keep different CMS.

The local IT director is the point person for cybersecurity, but the day-to-day operation is often deferred to a network administrator. There is a general belief that cybersecurity is identical to network security. While most network administrators are well qualified, few would have the insight to provide cybersecurity leadership. IT directors typically face two major challenges:

• Maintaining operation efficiency pressured by end users in editorial, advertising and marketing;

• Budgetary constraints. Cybersecurity is often treated as a line item under information technology and IT directors often have to fight for cybersecurity allocations unless there is an emergency.

Recommendation

CISO addition. The mirror has two faces. A Chief Information Security Officer is the reflection in the mirror for the IT director. The CISO is also the conduit and educator to implement EISP details. A full-time CISO should be added to the local C-suite team.

The IT director, if given both operating and guarding portfolios, may risk sacrificing one over another. In office politics, infrastructures win friends and prohibitions net foes. When push comes to a shove, IT directors will most likely be Santa than Scrooge.

Pitching to the board for this addition, we can analogize by using the stock market as an example. NYSE is the trading floor, but the Securities Exchange Commission is the watchdog.

2. Management process

About one-third of the newspapers in North America changed ownership through mergers and acquisitions in the last decade. Some deals resulted in bigger and stronger media empires while others were gobbled up by venture capitals raised in the name of technology.

The epic center on cyber activities is at the local level. While corporate may have policies such as EISP, many are misaligned especially with owners from non-media sectors. Corporate interventions are not timely enough to deal with the issues. Corporate works 9-5 while the newsroom 24/7.

Traditionally, newspapers were quite transparent in their operations as they believed in open and honest communications. Page two of most newspapers is devoted to admitting guilt. It's a strategic position to publish retractions, corrections, clarifications and apologies.

One might argue in the digital era the online editions have more influences. The trend is true but the print edition is still revenue important especially in non-metro markets. My former colleagues at the Poughkeepsie Journal just cheerfully reported that their Black Friday edition weighed 2.5 pounds and had 400 pages.

In the name of freedom of the press, the newsroom sees itself as the centerpiece and every other department including IT, advertising, production and circulation are there to support them as servants. If IT flags a cyber problem, the editors will insist the problem be fixed after deadlines. Fortunately, newspapers have daily deadlines and the fixes are still more prompt than those at many other companies.

Culturally, journalists see IT issues not their problems. And few of them can distinguish the difference between cyber and IT issues. They are also the ones who import cyber risks as they visit sketchy websites, insert USBs from "usually" reliable sources and receive news tips – real or fake – through emails.

The attitude is they are on the frontline to deal with urgent matters and if there is a problem, you at IT will fix it. Journalists are easy phishing and spear phishing targets even though they write about them all the times. They do not report problems unless their systems crash.

Recommendation

EISP review. At the corporate level, an EISP rewrite may be necessary to align cybersecurity practices with the media business. This may include standardizing EISP amongst different local newspapers. EISP has to have contribution from the frontline as they are first ones dealing with the issues.

A company-wide cybersecurity awareness program needs to be deployed.

3. Training awareness

Corporate executives often find it hard to argue with journalists as the later can write and debate better. Reporters and editors are also strongly backed by their boss, the editor-in-chief. Newsrooms have the largest user base followed by advertising.

At most newspapers, cybersecurity is mainly enforced through prohibition, such as:

• Authentication;

• Network segmentation;

• Email attachment limitations;

• Restricted internet access;

• Reporters filing remotely required to use VPN;

• Company laptops not to be connected via public networks, such as at hotels and internet cafes.

Although IT departments are up-to-date with server security patches, there are often time delays on workstations, as some apps such as CMS and graphics programs, may not be readily compatible.

Turf issues

• IT staff are trained to be firefighters and they deal with issues as they arise. They are more on the defensive. Disaster recovery practices are developed more along the lines of hardware failure and system backup.

• Newsroom users have the attitude of "Tomorrow is another day", once an edition is put to bed, so sleeps any cyber problems. Reporting is often neglected.

• Advertising executives care about revenue. Whether a client's artwork is successfully transmitted is more important than cleanliness.

Recommendations

Borrowing from Mark Twain, the de facto saint of American journalism, "continuous improvement is better than delayed perfection."

• News corporations need to have updated EISPs which encompass the different operating departments. Given the appropriate training, it's easier to turn an editor into a cybersecurity professional than make an IT guy into an editor. With a cybersecurity professional groomed from the newsroom ranks, the implementation will be sweeter swallowed as the new CISO will be seen as someone who understands journalism.

• The office of the CISO needs a budget. Unlike other departments, there is no ROI, instead the benefit is in the Return of Mitigation (ROM).

• Cyberattacks should be treated like diseases. If a user fears about an infection, treatment should be sought. Cyber clinics can be set up to deal with emergencies and fears.

• The most economical means in public safety is preventive medicine. In cyber health, the vaccine is awareness training and cybersecurity should focus on fire prevention rather than firefighting. Different departments need different training.

Cybersecurity is not just for some of us, some of the times; but all of us, all of the times. It carries a strong "Yes" message instead of a "No" like in the prohibition.

Protective technologies

Questionnaire and findings

The following questions were directed to the director of information technology who has responsibility over cybersecurity. The recommendations are based on measures that are already in place, and/or available products to remedy the shortfalls.

1. *Do you have cyber security awareness programs in place for different classes of users in the organization? Please provide details on the programs, such as training, frequency, refresher education, phishing and spear phishing prevention, training development and network administrator certification.*

   Findings:
   a) Certification for network and server administrators are mostly up to date but require central record keeping;
   b) Cybersecurity awareness training for non-IT staff is sporadic.
   Recommendations:
   A company-wide training initiative is needed.

2. *Do you have a cyber help center or clinic set up to allow for centralized incident reporting? If not, what methods do you use to help distressed users?*

   Findings:
   Cyber incidents are reported and logged the same as general systems problems;
   Recommendations:
   Cyber incidents should be triaged, logged and followed up by the office of CISO.

3. *When authorized users access your gateways – such as AD, VPN, remote access and internet portals – do you deploy multi-factor authentication? Please detail if native multi-factor authentication is available.*

   Findings:
   No 2FA or advanced password protocols are in place.
   Recommendations:
   a) When users access the systems remotely, 2FA to be required.

b) Complex password requirements to be implemented for in-house logins, all systems.

4. *For workstations at operating departments, what protection measures are deployed? Please provide details on the logistics of OS upgrades and security patches, application upgrades, SaaS application access, anti-virus software, restrictions on external devices (such as external hard disk and USB drives), restrictions on user-installed applications and file sharing protocols.*

   Findings:
   a) Anti-virus software is installed on all workstations;
   b) System upgrades are pushed out after deadlines;
   c) No policies in place on BYOD or external devices.

   Recommendations:
   a) BYOD only allow connections to segmented portion of network.
   b) External devices to be scanned first at standalone IT scanning stations.

5. *What policies have you set for incoming and outgoing SMTP servers? For outgoing, please detail limitations on recipients per hour, recipients per message and maximum message size. For incoming, detail limitations on maximum message size, disk space allocation for each mailbox and attachment type limitations, spam filters and suspicious mail quarantines.*

   Findings:
   Corporate email policies including quotas and file limits are observed.
   Recommendations:
   No action required.

6. *Do you allow editors, reporters and advertising executives to remotely access your system via their devices using public networks, such as at hotels, press conferences and internet cafes? If your answer is "no", how can they access?*

   Findings:
   No policies in place. Connections not monitored regardless of locations.
   Recommendations:
   All users connecting remotely be equipped with dedicated wireless modems connected through cellular data network.

7. *Do mobile devices – including laptops, phones and tablets issued to reporters – have disk or file encryption enabled?*

   Findings:
   Yes, if company issued and configured.
   Recommendations:
   Non-company issued or configured devices be allowed only connected to segmented network.

8. *For the Content Management System, including newswire and local contents, is file encryption enabled in the configuration? Please provide details on the deployment, i.e. 128- or 256-bit AES encryption.*

   Findings:
   256-bit AES encryption deployed.
   Recommendations:
   No action required.

9. *For file servers, are hardware encryption deployed and facilities physically secured? Please provide details on data backup setup – such as off-site servers or cloud storage, levels and methods of encryption, and site access control.*

   Findings:
   Yes. Data back up to cloud.
   Recommendations:
   Main storage to be migrated to cloud.

10. *On network and cloud protection, what measures are in place to protect traffic in and outside of the firewall? Please provide details on network traffic benchmarking, analytics tools such as machine learning and DDoS detection software, escalated defensive procedures, and router configuration.*

    Findings:
    No measures in place.
    Recommendations:
    Migration to scalable cloud to automated defense against DDoS.

Legal considerations

Our newspapers in our region serves readers in New York, New Jersey, Connecticut, Rhode Island and New Hampshire. We also have online subscribers who live in Canada and Europe. We are aware of most of the different federal, state, municipal and foreign regulations governing our business operations. However, they are scattered and unorganized.

Cybersecurity Policy Chart
It is recommended that we develop and publish a Cybersecurity Policy Chart modeled after the CSAIC's DoD Cybersecurity Policy Chart. At a glance, this chart will enable our organization to identify the statutes and regulations that govern our cyber activities. Unlike the government charts which outlines all the links among the different government agencies, our chart also needs to reflect the links to our suppliers and contractors. This will enable us to quickly shut off any valves in the event our external partners report a breach.

Law enforcement and ISACs
We need to identify the government agencies that we are required to disclose the information to as well as Information Sharing and Analysis Centers (ISACs) we can share information with and what type of information we can safely share.

Chain of command
An organization chart listing the chain of command including officers, executives and professional personnel needs to be filed with the governing board of directors.

Playbook
A playbook outlining step-by-step procedures we will have to follow in the event of a cyber incident needs to be published and circulated among the C-suite team and operation managers. The procedures should cover:

- Escalation procedures
- Law enforcement reporting
- Disclosure to affected parties
- Media announcement
- Notification turnaround time.

Insurance
We need to mitigate the bulk of the financial risks by leveraging liabilities with dedicated cyber insurance policies. An independent actuary professional needs to be hired to calculate our exposures in the following areas:

- Loss of business
- Equipment replacement
- Disaster recovery costs
- Overtime labor costs
- Legal bills
- Third-party liabilities
- Government fines
- Compliance oversights
- Reputational harm

Communication protocols
We are in the business of communications, but it doesn't mean that we are good at it. We must have in place internal and public communication procedures to mitigate any unnecessary anxiety. A PR firm needs to be retained.

Financial
In our operating budget, we need to include cybersecurity contingency, such as approval limits, cost centers and supplementary allocations. The CFO needs to include this in the next annual budget. For future capital projects, cyber contingency costs need to be factored in.

Supply chain management
In our procurement process, we need to incorporate the following procedures:

- NIST's Information and Communication Technology (ICT) Supply Chain Risk Management (SCRM) NIST SP 800-161
- ISO/IEC 27036 on IT outsourcing and cloud computing services.
- PCI-DSS for acceptance of credit card payments
- GDPR for general data protection regulation compliance

Helping under-qualified vendors

Many of our vendors were chosen because of the performance and quality of their products, but they may not have up-to-date cyber risk mitigation policies in place to protect their customers. We need to implement measures to ratify the situation, such as:

- Reviews of existing contracts
- Future contractual considerations
- Publication of procurement guidelines
- Financial incentives for vendors to be in compliant
- Establishment of a third-party management committee

Supply chain matrix

We need a matrix outlining the following details:

- Services
- Vendors
- Audit procedures
- Contract commencement date
- Contract expiry date

Incident response plan

As a news media, with web publications and newspapers distributed in multiple states in the Northeast, our digital assets are deposited on both sides of the firewall. Emails and business systems are managed under another corporate domain and are not discussed in this plan.

Local area network and servers behind the firewall host editorial, advertising and production services.

Content management systems (CMS). Depending on the type and sources, assets are managed through various CMS behind the firewall. Key CMS include:

- Editorial
- Advertising
- Prepress
- Graphics and pictures
- Videos and soundtracks
- Newswire
- Archives

Gateways manage the intake of information, including files from reporters, newswire services, press releases and readers' input. Trusted users and wire feeds are allowed access to CMS while others are deposited on servers in the DMZ.

Web publications are hosted on web servers outside of the firewall and available to the public.

Preparation

Newspapers have a 24-hour life cycle and "tomorrow is another day" is the mentality of the industry. We have enemies from inside and outside: nation states, politicians – even our own, angry readers, and disgruntled employees – past and present.

Other than just keeping the systems running, IT has traditional been charged with protecting the digital assets. Knowing pressmen do not double as security guards, management now realizes that IT should not be the cyber guards.

A culture is being cultivated that we need dedicated cyber security preparation and the effort is everybody's business all of the times. An incident response guide is prepared, response teams are identified and semi-annual reviews are planned. Data is also backed up to clouds.

Risk mitigation cannot be easily outsourced in our business, but the cost for recovery in the event of a loss can be offset by dedicated insurance policies. An insurance review is underway.

Planning

Cyber protection is everybody's business and roles have to be clearly defined. The plan is to involve everybody in the organization and training will be based on stakeholders' responsibilities.

A playbook is to be published outlining reporting and response procedures.

The governance structure is defined and tasks are identified.

- Leadership: This includes the board of directors, legal counsel and the C-suite team. They are to approve the cyber response plan.
- Crisis management team: This is command central in the event of a major incident. The team includes the CISO, CIO, network administrator, legal counsel and representative from editorial, advertising and prepress departments. This team is responsible for developing the playbook.
- Red and Blue teams: These are ad hoc teams drafted to perform simulated wargames as part of the semi-annual reviews. In the event of an attack, they will also rotate into defensive shifts.
- Operational managers: They are to be trained on how to keep the operations running in the event of a cyber incident.
- All employees: A cyber security awareness training program has to be delivered to all on an annual basis.

A communication plan covering both internal and external targets is to be published. Spokespersons are to be designated.

Preparation

The office of the CISO serves as the reporting center for all cyber incidents. This avoids arbitrary delays caused by department heads. To protect whistle blowers, it is written into the company's standard operation procedures that ALL suspicious cyber activities are to be reported promptly first-hand to the CISO's office through email, phone calls or personal presence. All reporting incidents are logged and investigated using a check list.

A cyber response kit, a.k.a. the jump bag, is created and stored offsite. The kit is to be used to carry out forensic work in the event of an attack. The kit contains a printed copy of the playbook; a list of all users of the Active Directory; a fully configured Apple laptop loaded with Mac OS, Linux and VMWare Fusion operation systems and the common desktop applications used by the CMS; CMS configuration files; USB storage; note pads; digital camera; connecting cables; and a wireless cellular modem.

Two ad hoc strike forces, the Red and Blue teams, are to be formed to conduct cyber wargames at least once a year to stimulate penetration and defense tactics. The findings are to be included in the annual cyber review. Team rotations are encouraged.

Tools

An external cyber security consulting service is retained to provide third-party advice in the event our own team cannot resolve an issue. We also subscribe to an external monitoring service to help flag unusual network activities. On a day-to-day basis, we deploy the following tools to detect cyber threats:

• IPDSs are installed and configured to monitor network traffic and node activities;

• Triggers are set up in system and application logs to flag administrators;

• Anti-virus software is installed in all nodes including servers and workstations;

• Firewalls and encryption technologies are used to protect networks and files, alarms configured to flag unusual activities;

• Network analytics are used to early detect cyberattacks;

• Vulnerability scanners are run daily to detect new risks;

• Unauthorized vulnerability scanner users are investigated when flagged by system monitors.

To keep our teams up to date about new threats, we exchange information with our peers through intelligence forums.

Analysis

Once an attack is identified, we need to understand the battlespace. The CISO's office should determine whether the attack affects systems outside or inside the firewall. Is foundation data at risk? Network analytics and logs should give a quick glimpse on what is affected.

If the attack only affects access to published web pages, it's most likely a DDoS. Escalated surveillance measures, such as detailed system log, may have to be deployed to further monitor gateways and ports. Affected web pages or sites may have to be inventoried and out-of-service impact measured.

If the attacks have made their way through the firewall, all CMS logs should be examined to see the scope of the attack. The types of attack – such as data breach, network breach, malware or ransomware attack – also have to be identified.

If automated IPS stoppage has been triggered, the threats may have been temporary contained.

Newspapers have nightly deadlines. Depending on the time of the day, a decision will have to be made whether to ride out the attacks until after deadline or can a fix be deployed fast enough for products to still make deadlines.

All decisions should be based on outcomes of a pre-determined checklist.

Containment

DMZ

While massive botnet attacks are already protected by our private cloud technology by blocking DDoS across layers 3, 4 and 7, protecting the network, transport and application layers. The technology stops all sizes of DDoS attacks from massive botnet assaults to single malformed packet DoS attempts. In the event of an attack, the cloud will scale the bandwidth dynamically with no user intervention required. An alarm will be sent to the CISO and network administrator as this happens. This service is provided by a third-party supplier.

In the event if the technology fails, we can still resort to the basic Captcha gate method, although not the best, it will at least distinguish between a computer and the human.

Behind the firewall

Inside the fences, if an attack is verified, our first task is to identify and contain the attacks, avoid any further lateral movements of the virus.

The goal is to continuing provide un-interrupted services for the CMS. Certain automated functions may be disabled. Some non-essential systems will be shut down or taken offline.

If workstations are infected, they are taken offline.

Backups of infected systems will be recorded onto standalone storage devices for future forensic investigation.

For the public

As a newspaper, we are in the communication business. We are usually good at it except this time we are in the the receiving end of the message.

When dealing with the public, to remain impartial, we may still want to enlist the help of a public relations firm. They have the established contacts of different media types. Also, during the defensive battle, our chief spokesperson, the editor-in-chief may be extremely busy with production while having limited computing power. The editor should still be available for some key interviews.

As a newspaper, we will uphold the principle “the public has a right to know” by not withholding any information. Press releases will issued be daily.

For the staff

During a cyber incident, our own staff should also be well informed about the battle scene. This will avoid any unnecessary anxieties and rumors. The best persons to provide this type of messages are the trainers who originally deliver the cyber awareness training sessions. They will have the trust of the staff as a bond has already been established.

For the board and Wall Street

The governing body as well as the public investors should be given updates on a daily basis before the market opens. This will avoid unnecessary fluctuation of stock prices and any possibilities of insider trading incidents.

For the authorities

In the playbook, a cybersecurity-related policies and issuance chart has already listed at a glance all regulatory agencies we have to file incident reports to.

Eradication

During the attack, a decision has to be made whether to ride out the attacks until after deadlines or to do an on-the-go cleanup. The decision has to be based on if the cleanup actions risk further deterioration of the situation. Follow the decision matrix in the playbook to determine the action.

During the cleanup, priority should be given to networks, servers and CMS:

• Tools will be used to remove malware remnants from all servers with automated malware cleaning and repairing functions to minimize re-infection;

• Scans and remediates compressed archives for malware to avoid unnecessary decompression;

• Further detect gaps in the security system by triggering and monitoring an in-depth vulnerability scanning;

• Isolate accounts that were used as carriers of the attack;

• Re-configure firewalls and apply system patches;

• Consultation with industry peers and see if they had similar experiences.

Individual workstations and laptops should also be scanned once servers are secured.

Recovery

When the fever cools off, it does not always mean the disease is cured. Damage assessments have to be made to determine if it's just a relief or the system has been restored.

Very seldom would a repaired system can be restored to its original health. A decision has to be made if a restoration from cloud archives is feasible or necessary.

The risk of restoring from historical retrospect archives is it may still bring back the same problems if the malwares have been hiding in the system for sometimes.

The rule is to restore only data files while software apps should be reinstalled fresh with vendor's latest patches.

The process to restore and rebuild should be planned and segregated by functional departments and their systems.

Schedule system restoration.

Post-event analysis

When the battle is finally over, the warriors are tired. However, a post-mortem has to be performed soon as to avoid any memory loss and the incidents from repeating again.

Its starts with the CISO team first analyzing the events. A chronological timeline may have to be recreated to account for the different events. The evidence archives stored on standalone servers should be analyzed. It may worth the while to send the data to the software vendors for diagnosis.

A report is to be drafted by the CISO and approved by the C-suite team. The report will continue to flow upstream to the board of directors, legal counsels and insurance adjusters for claims.

All regulatory bodies involved should be notified with an incident report within the required filing period.

A revised cyber protection plan has to written into the next semi-annual review.

Tel: +1 519-673-7333 | **Email:** ctse@qint.com