clearswift

Preparing for a Cyber-Breach

Forewarned is Forearmed

June 2016

Contents

Introduction

There are enough cyber-security stories in the media to realize that a cyber-breach is highly probable. It is no longer a question of 'if' but 'when'. In fact, the likelihood of a cyber-breach occurring is so predictable now that we are seeing the rise of cyber insurance and cyber risk management organizations that can forecast a potential breach with greater than 90% accuracy.[1]

Many organizations struggle with this fact and so end up doing nothing about it; when a small amount of upfront effort can make the situation, in the event of a breach, less damaging to the organizations stakeholders and significantly easier to manage.

This paper will help organizations prepare for a cyber-breach and provides an outline plan to help cope with the situation. A plan will prevent panic – the last thing needed while undergoing a security incident.

Why you need a cyber-breach plan

Perhaps the easier question is, 'why do you think you don't need a cyber-breach plan?' You probably have plans for other types of disaster, from the simple fire drill through to disaster recovery and business continuity plans. Today a cyber-breach can be far more damaging to the long term viability of an organization than traditional disasters. Long-term damages can have a ranging impact from stock value, to fines, to loss of customers. In fact, research shows in the retail industry alone 36% of customers will shop less frequently and 12% of shoppers will stop doing business altogether with organizations that were hit with a breach.[2]

But being prepared with a plan to technically contain the breach is just the beginning. The crisis management work of preparing for required customer notifications, potential lawsuits and repairing reputational damage will require some intense work under pressure. New global regulations, such as Japanese MyNumber, HIPAA (Health Insurance Portability and Accountability Act), FCA (Financial Conduct Authority), PCI DSS (Payment Card Industry Data Security Standard) and GDPR (General Data Protection Regulation) being introduced by the European Union, are more formally increasing this pressure with requirements to have such notifications delivered within 72 hours of the breach. You need a plan.

Scenarios (or types of event)

In the cyber-security arena there are multiple types of event which can occur, this can range from a simple virus infection to a Distributed Denial of Service (DDoS) attack, from a lost laptop to a hacker who has stolen the whole customer database. You probably have procedures for dealing with some of these already; a virus outbreak is unlikely to require the plan to be put into action, that will of course depend on the severity. A malware outbreak at the Gundremmuingen Power plant required the site to be shutdown[3] – but it is worth listing the events and then stating whether the plan is required or not.

Scenarios can include:

- Traditional malware/virus outbreak
- Ransomware infection
- Lost laptop
- Lost media – USB sticks, CD ROM, DVD, etc.
- Stolen systems / servers
- Denial of Service attack
- Web site hack (including website defacement, information stolen, website serving up malware)
- Data breach through a malicious hack or a malicious insider (including from databases or through documents and reports)
- Data breach from an employee mistake, e.g. sending critical information be email to the wrong person or accidentally publishing on corporate website
- Data breach from a third party data processor

The scenarios can then be applied to various business units and individuals or groups, in conjunction with the critical information they are responsible for, or have access to.

Creating a list of scenarios enables the organization to prioritize based on probability. A risk management framework, or plan, is then developed to address the scenarios where there is the greatest risk and can then be expanded over time to reduce the overall risk and help mitigate the impact of further incidents.

[1] KING, R. (2016). *Cybersecurity Startup QuadMetrics Calculates Odds a Company Will be Breached.* Dow Jones & Company, Inc. Retrieved from http://blogs.wsj.com/cio/2016/01/12/cybersecurity-startup-quadmetrics-calculates-odds-a-company-will-be-breached/

[2] Perceptions, R. (2014). *Retail's Reality: Shopping Behavior After Security Breaches.* Retrieved from http://www.interactionsmarketing.com/: http://www.interactionsmarketing.com/retailperceptions/2014/06/retails-reality-shopping-behavior-after-security-breaches/

[3] www.techworm.net/2016/04/german-nuclear-power-plant-shut-due-malware-chernobyls-30th-anniversary

Where to begin

All too often projects never get started because at the outset they look too tough to complete. You don't have to do this alone, there are others who can help. This could be 3rd party consultants or a trusted partner or supplier who can help with an initial workshop (if you want to keep costs down) or be there throughout the duration of the project. If you are not sure of the regulations which you may be subject to, then it would be a good idea to get someone in to help, it will save a lot of time and effort researching them. After making the effort to start, the project will likely turn out to be more manageable than expected. In essence there are three key things that need to be understood and done when an incident occurs:

- Follow the plan (hopefully you will have tested it before the event – so you know it is going to help)
- Get people prepared and moving
- Communicate effectively through each phase of the plan implementation

After this - the rest will follow.

The 'Cyber-Breach Team'

Before you build the plan, you need the people. Creating the plan with the people who will actually be involved makes disseminating it easier. The question is, who?

Cyber-breaches will fall into two simple categories, major or minor – and you won't know which one it is until after it has happened and the initial analysis is carried out. For this reason you need to assume the worst. So, the key members of the team should be:

- CEO – this is the face the media will want to see
- CIO (or equivalent) – the breach will be about IT and / or critical information
- Marketing – the marketing team will be needed to handle communications in all forms
- Legal – there are potentially lawsuits here, so bring the legal team in early
- Sales – if this hits the front page of the news, then sales will be impacted
- Support – as per sales, customer facing roles need to be involved

Communications and legal notifications

As with any serious incident, there is a need for communication and a cyber-breach is no different. In the case of customer data loss, legal notification requirements must be complied with at a local, national and international level. In fact, research conducted by The Ponemon Institute in the United States showed how likely formal notifications were required:

- 95% of businesses suffering a data breach were required to notify data subjects whose information was lost or stolen
- 97% were required to notify under state statutes
- 58% were required to notify under federal privacy acts such as HIPAA and GLBA[4]

For those outside the United States the statistics on notification are less well understood. The new EU General Data Protection Regulations (GDPR) which come into force in Spring 2018 are formalizing the need and process of notification such that such statistics will become more readily available. As GDPR impacts anyone who does business in Europe, for example a US company notifying EU citizens, not only those with a presence, it will create a need for a breach notification process which can cross continents.

There are different people who will need to be communicated with, having the plan list them out ensures that no-one is missed. Communications will need to be prepared for (potentially) the following groups:

- Employees
- Customers
- Suppliers
- The Board
- Shareholders
- Regulatory Authorities
- The Media

[4] Ponemon Institute. (n.d.). *The Business Impact of Data Breach.* Retrieved from Scott & Scott, LLP: http://www.scottandscottllp.com/main/business_impact_of_data_breach.aspx

Step 1 – What?

An incident has occurred. Bring the team together to discuss the plan as soon as possible. Even if very little is known there will be the need for communication.

The critical first step is to better understand what happened and who is impacted. Only when this is complete will it be possible to determine what the next course of action is. If this is a minor incident then it might not be necessary for the CEO to be the spokesperson, that baton may be passed to the CIO or to Marketing.

What actually happened?

It's hard to communicate if you don't have the facts, even if they are thin on the ground. Find the facts and ensure everyone who needs to know them does. At this point having conflicting stories will be even more damaging (which is why it makes it easier to just have one spokesperson.) Ensure that the communications to different groups remains constant.

There will probably need to be a secondary team here who are going to investigate what actually happened in order to answer the next questions – what information was involved and how many people are impacted?

What information is involved?

What critical information was involved? Is this about customer records with credit card details or stolen product plans? This is important to understand for many reasons, including breach notification and general communications.

How many people are impacted?

Are we talking about one person or a million? While all critical information is important, the plan for dealing with a small breach versus a large will be different. Do you need to reach out personally to the impacted parties, or take out a full page advertisement in newspapers?

Information means money, but some types of information are more readily used for fraud than others. Particularly payment card or bank details. If this information is compromised, then it is even more important to notify the individuals and where possible their banks, at the soonest, that the incident has happened and to monitor for fraudulent behavior.

Step 2 – Inform and mitigate

To get through a security incident with the minimum of impact, there is a need to get the whole organization behind the response. Keeping employees well informed will reduce the ruinous impact of rumors. Create a project office and let people know where it is and who is on the team. Who is it they need to direct queries to, keep it streamlined, or if they have questions themselves? Direct them towards an Intranet site where updates will be posted and current.

Communicate

From the plan there will be a list of people and / or groups which need to be communicated with. These can be prioritized based on the incident and the appropriate messages sent out. The sooner the communications happen, the quicker concerns will be dissipated.

For some security incidents, there is a need to issue a breach notification notice. The time to issue a notice will depend on the legislation and the region.

Different groups will require different communications, and a different frequency of communication. The key to a successful communication schedule is to carry it out on time, and even if there is no news to communicate then let this be known that this is the case. While it may appear trivial to delay communication until there is news, for those waiting, it is reassuring to know that they haven't been forgotten.

The Media

There is a saying, 'that there is no such thing as bad press'. Unfortunately when it comes to a security incident, particularly a data breach, this is not the case. Defining a spokesperson and a set of guidelines on what can and what cannot be said to the media will be essential. Facts. Keep the facts straight and don't speculate – as the media could take rumors and speculation and use it to their advantage and your disadvantage.

Has it stopped yet?

In general the question most people want to know the answer to is, 'whether the problem is over, or is it ongoing?' This might not be immediately answerable, in which case try and give a timeline for when more information is to be made available.

What was the weakness that was exploited and has it been resolved? If systems were compromised, have they now been cleaned? Was there a back door which has now been blocked? Has the information been found on sites on the Dark Web, known to be used by cyber-criminals?

If there are steps which can be taken to mitigate the breach, ensure that they are taken. For example, taking the website offline for a short period of time. Or resorting to a manual process to take orders.

FAQs

Depending on how many people are impacted you may want to consider publishing a 'Frequently Asked Questions (FAQ) document' on your website. This will alleviate the strain on the phones as people will have somewhere to go to get an update and again, will act as a one-stop-source of information.

Update the FAQ regularly, even if it is to say there is no new information – at least people know you are trying your best.

Step 3 – Ongoing

Unlike a fire alarm, where people return to the building and continue as if nothing has happened, this is not the case with a security breach. The impact of a breach can last for years and will often last for many months.

Ongoing impact

The impact of a severe breach should not be underestimated, along with fines, there will be reputational damage. Existing customers will potentially leave and could sue you in the process, and gaining new customers will become more difficult.

Regulatory authorities will not just fine you, but will probably insist on enhanced yearly audits as well as putting in place measures to prevent a breach occurring. When building a plan, take these components into consideration in order to minimize the impact.

Where there is an opportunity for fraud, such as compromised bank account or credit card details, plans will need to be put in place for credit monitoring; deciding which organization will be used and for how long, will make the implementation quicker and easier.

Minimize the impact

While there are lots of groups which can be involved, it is your customers which need to be protected the most. Protecting your customers will help protect your reputation. Being seen to do right by your customers will help you regain their trust and remain with you over time.

Customer support will be overwhelmed with calls from concerned customers. Having a plan to increase the resources available is important. Will these be internal people, or an external agency? Will you need more phone lines or desk space? Will there need to be some training as to how to handle the situation and what to say? Can this be done in advance of any incident? Do you have a timeframe in which the enhanced support desk can be up and running, for example two hours?

As well as telephone support, social media and your website can be used. In the case of your website, there is the potential for an excessive amount of traffic, so there may need to be a plan to increase capacity and the bandwidth to manage it.

During the incident, it will not be business as usual, but the goal will be to return to this state for as much of the organization as quickly as possible. The IT department will take the longest to return, as there will be additional processes and monitoring which will need to be adhered to.

After the event, remind customers what you do best, create promotions to keep them as customers and reassure them that you are doing everything you can to prevent an incident in the future.

Ensure it won't happen again

While nothing is guaranteed, there is a need to prevent the same incident happening twice. Steps should be taken to not only prevent the incident, but also to prove that the incident won't occur again. This can include improved education and awareness for employees, better processes, regular testing, and policies and the appropriate technology to underpin your security.

All too often an incident occurs and steps are taken to prevent it from happening again, which is good – but look at the bigger picture and take the opportunity to see where the real failings were. Fixing the root cause of the problem will help in the future, when a different type of breach might occur. New business practices need to be looked at from the perspective of a cyber-breach and potentially stopped as the risk is too high. There are a myriad of cloud collaboration tools to share information – but which ones meet your security criteria? This doesn't mean stopping their use, it does mean, however, being able to use selected ones securely. Create a list of what is, and what isn't, approved. Shadow IT is often rife and the CIO or IT department don't know about it until it's unfortunately too late.

Revisit the plan

The plan needs to be continually revisited, not just in light of an incident, but also in conjunction with media stories of new cyber-attacks. With the newly reported attack, does the organization have suitable defenses in place to prevent the attack from having the same impact within your organization? If not, then a plan needs to be put in place to improve the protection of the critical information.

Reward

A good response to a security incident can save the company and so consider recognition and/or a reward to those who have been involved.

Prevention IS better than cure

While the prevention of security incidents is not always practical, there are a number of preventative steps which should be taken:

- Which business processes are least secure? What ways can they be improved?
- Does IT have all the resources needed to help prevent an incident or to respond appropriately in the event of one?
- How can the culture of the organization be changed to move it towards one of protecting critical information and systems? This is a continuous process, not a one-off and will evolve as the business changes. Think about how cloud collaboration and sharing of information has brought benefits, but also potentially created new risks which need to be mitigated against.
- Are the existing information security policies adequate for today's threats?
- Are existing policies consistently enforced? Or is there a need for improved technology to do so?
- What other measures can be put in place to monitor for a security incident and to prevent or minimize the impact?
- Test the plan. It's all well and good having a plan, but if it hasn't been tested then you don't know how it might be improved. Often it is the little things which need to be updated, such as new team members or phone numbers for people on the team.
- Keep educating employees, especially any new-hires, and make them aware of both the plan and of the risks that are being faced. Ensure they know what to do if there is a cyber-breach and the process to follow. Communication shouldn't start with an incident!
- Look at cyber-insurance. It might not be worth it for you, but if you haven't looked then you won't know. This is a relatively new field, but it can help with some of the incurred costs, especially for a small business.

Effective security is about building layers of protection, each layer needs to be regularly assessed and, if required, improved.

Summary

The chances of a security incident, including a data breach are now sufficiently high that it is a case of "when", not "if". The key to dealing with an incident is to be prepared, as this will minimize the impact. Minimize the impact to customers, employees and prospects. Minimize the impact to the organization, its Board, Executives and staff.

The key to preparation is a plan, start with a simple outline and some simple scenarios and then build upon it. Scenarios can be taken from media stories, not just for validation but also for improving the plan. Understanding the risks and consequences will help focus the mind. The biggest issue organizations have is to prevaricate and not to start planning as they don't believe it will happen to them. This is a false economy.

Forewarned is forearmed.

Appendix A: Cyber-breach plan template

The basis for this template is not that different from a disaster recovery / business continuity plan. If you have one of these plans, then look to use that as the initial baseline.

Some items in the template for action can be completed before the breach occurs, others will need to be completed when the incident occurs and as the specific details become known.

Task / Activity	Comments
Cyber Security Event Team	List of personnel who will be coordinating the response to the cyber-incident. • CEO • CIO • Marketing • Sales leads • Customer support
Spokesperson	Depending on the severity of the incident, the spokesperson will either be the CEO or a regular spokesperson, for example the Head of Marketing. Ensure there are guidelines on what can and what cannot be said, to whom and when.
Communication groups	Who are the groups you need to communicate with? Including employees, customers, shareholders and the authorities.
Incident response	Determining the response to the incident will depend on the answer to the following questions: • What actually happened? • What critical information was involved? • How many people are impacted?
Communication plan	What groups and frequency of communication is required? Are there outline communications which can be created ahead of time?
Authorities / Legal Notifications	What authorities need to be informed (based on the information compromised)? Are there time limits for breach notification notices to be sent out?
Credit monitoring	If required, which organization will be used for credit monitoring and for how long? (typically 12 months). Are there any other long(er) term mitigations which are required?
Incident stopped	How can you tell if the incident is over? How will this be communicated?
Additional resources	Will there be additional resources available to help with customer support desks? Will this require additional space, equipment, etc.?
FAQs	Will you create and publish FAQs? Where will they be published? Who will take the lead? How often will they be updated?
Ongoing tasks	Who will be responsible for ongoing tasks, including monitoring to ensure mitigation plans are working as required? What is the timeline for implementation?
Scenarios	What are the scenarios and quantum of breach (one record or a million or somewhere in between) which will create the response?
Prevention	Are there steps which can be taken to mitigate the impact of a breach? These can be prioritized and implemented as time and budgets allow.

clearswift

Clearswift is trusted by organizations globally to protect their critical information, giving them the freedom to securely collaborate and drive business growth. Our unique technology supports a straightforward and 'adaptive' data loss prevention solution, avoiding the risk of business interruption and enabling organizations' to have 100% visibility of their critical information 100% of the time.

For more information, please visit **www.clearswift.com.**

United Kingdom
Clearswift Ltd
1310 Waterside
Arlington Business Park
Theale, Reading
RG7 4SA
UK

Germany
Clearswift GmbH
Im Mediapark 8
D-50670 Cologne
GERMANY

United States
Clearswift Corporation
309 Fellowship Road
Suite 200
Mount Laurel, NJ 08054
UNITED STATES

Japan
Clearswift K.K
Shinjuku Park Tower N30th Floor
3-7-1 Nishi-Shinjuku
Tokyo 163-1030
JAPAN

Australia
Clearswift (Asia/Pacific) Pty Ltd
Level 17 Regus
Coca Cola Place
40 Mount Street
North Sydney NSW 2060
AUSTRALIA