Cyber Security Awareness
What boards and executives need to know

01 Security Matters to the Executive Team
02 Data Custodianship and Corporate Liability
03 Creating a More Secure Company Culture
04 Leveraging Security Research as a Business Strength
05 Weathering the Storm of a Security Incident

Originally published as a blog series on the Rapid7 Community during National Cyber Security Awareness Month, October 2014.
SECURITY MATTERS TO THE EXECUTIVE TEAM

Why is Cyber Security a C-level Issue?

The economics for cybercrime are shifting, creating a great deal of opportunity for attackers. To start with, the technical skills requirement is decreasing as malware and attacker tools become commoditized. This makes it easier for even unsophisticated attackers to succeed. At the same time, adoption of technologies such as smart phones, cloud apps, and social media makes every user in your network a potential weak point that an attacker could target to gain a foothold.

In addition, the strengthening of shadow financial systems has increased the potential for monetizing stolen information. There are abundant “black-markets” though which attackers can sell stolen credit cards, healthcare information, intellectual property and just about anything they are able to steal. Combined, these factors are lowering the barriers to entering the market, increasing the potential pay-off, and increasing the numbers of state-sponsored, corporate espionage, organized crime, and opportunistic cyber-attackers.

In this environment, it’s not surprising we frequently see breaches make headlines. A recent report from the Ponemon Institute claimed that 43% of businesses suffered a breach in the past year alone. Included, were some very high profile names – Target, eBay, JPMorgan, Home Depot – but you don’t have to be a huge billion dollar organization to fall victim to a cyber-attack. Even if you don’t attract the attention of a focused, targeted attack, there are plenty of opportunistic criminals launching untargeted, broad reach, “drive by” attacks that could affect your business. Remember, criminals have a ready market to sell your information. They don’t need any other reason.

The recent spate of breaches have revealed many lessons for anyone leading an organization. The first critical lesson is that regulatory compliance, such as PCI or HIPAA does not ensure security. All of the brands mentioned above were subject to, and compliant with, security regulation of some kind. It didn’t stop them from being compromised. Executives need to recognize that compliance does not equal security and checking the box is no longer sufficient.

Another lesson learned from these breaches is that it is critical that your organization is able to quickly detect and respond to security incidents should they occur. It’s not enough to just focus on prevention as a truly motivated, resourceful attacker will find a way in. You will be judged on how your organization responds and protects its customers and users. Ensure your organization has the tools it needs to detect breaches early, and processes in place to respond should an incident occur.

Speaking at a conference in July, the US Secretary of the Treasury, Jacob J. Lew focused on the increasing importance of cyber security, stating:

“If you are the leader of a business, you should know how strong your company’s defenses are, you should know if there are response plans in place in case a significant security breach occurs, and you should be getting regular reports on cyber security threats and what your company is doing to respond to those threats.”

The concept of liability for breaches is changing. Following the Target breach, both the CIO and CEO exited the company. There’s been speculation that there was more than just the security incident behind the CEO’s departure, but it seems to have at least been a contributing factor. Since the breach, the retailer has also faced a Congressional investigation, lawsuit from the financial sector, stock market dips, and has failed to meet its earning expectations. Target has demonstrated that being breached is not just a security risk, it’s a risk for the business as a whole, and needs to be taken seriously at the executive level.

The National Association of Corporate Directors offers several worthwhile resources for board members or executives who would like to learn more, including what kinds of questions they should be asking their team. One you might want to read is the “Cyber-Risk Oversight Handbook.”
When choosing to keep data, we have a legal and custodial responsibility, because we do not own that data. As a result, keeping data introduces an element of liability for your business, and protecting it is expensive and complex. Inventorying and eliminating regulatory data reduces liability, saving time and money.

Imagine hiring a babysitter for the first time, and they show up five minutes before you are scheduled to leave the house. No prior communication, no advanced information requested – and now you’re worried you’re going to be late.

"Hey there, I’m here - have a good time tonight!" the sitter says walking in the door and sitting down on the couch.

That’s it!? “Do you care to know the number of, ages and names of our children? If there are any special needs, medical issues, habits, dietary restrictions, bed times, or the last time they ate? Do you need to know when we are coming home, or how much we are paying?”

There is a very clear difference between the concerns and interests of a parent and this babysitter; those differences nicely illustrate the decisions companies make unintentionally when handling sensitive and regulatory data. Unlike babysitters, enterprises may have the luxury of choosing what responsibility we inherit. As corporate decision makers, we have the option of not storing data.

The holy trinity of misunderstood data is PCI, PHI, and PII.

- PCI is information relating to the Payment Card Industry – think of credit and debit cards.
- PHI is Protected Health Information, as defined by the Health Insurance Portability and Accountability Act (HIPAA).
- PII is Personally Identifiable Information – also under HIPAA.

Said again differently – companies are hesitant to destroy data, but retaining certain kinds of data involves expensive protection in the face of very real liability. More often than not, a very expensive decision to retain regulatory data is made without knowing what is at stake, often at a business level unacquainted with the associated costs and risks.

The current pervasive thinking is that gathering data creates “business intelligence,” which enables the business to operate more effectively and build new or stronger lines of revenue. Unfortunately, this data also attracts criminals who know they can turn a healthy profit for this stolen information on the black market. Defending against these attackers is time-consuming, expensive, and extremely challenging.

Attackers cannot steal data you don’t have, so eliminating specific data sets can massively lower your liability and reduce your expense.

A solid business case review makes sense. Some data must be stored for a period of time. Some abstracted data can provide business and market intelligence. Custodianship drives us to make informed decisions and to be deliberate about the investment required to protect data the company does not own.

By choosing to retain this data, we choose to retain risk and liability; your company will be held accountable for success or failure in safely caring for this data.

Keep only what you really need. Make sure whatever you need to run your business is vigorously protected.

And we strongly urge you to look into what liability protection you have around security threats. You may think you’re covered and actually find that you are not.
As a business leader you probably do a great deal of work on the road or at remote locations, as do many of your employees. While mobility increases productivity, it greatly increases the risk of data loss to your organization. Virtual workplaces are abundant: Homes, coffee shops, restaurants, airports, and other public locations all serve as convenient remote offices. Unfortunately that means that employees are accessing company information from insecure networks—but in many cases, they may not realize why or how their behavior increases liability for you, their employer.

Uninformed employees are a significant risk to the organization, risk that can be managed with security policies to clearly outline what behaviors are (or aren’t) acceptable from a security context. Policy is an effective educational tool, behavior deterrent, and in some cases a first-line defense against employee-induced risk to the business.

Employees are stewards of corporate data — they need to be trained and empowered to work safely and efficiently.

Why policies?

A security policy is critical to protecting corporate assets. The consequences of insufficient organizational security can be substantial: Security breaches, loss of sensitive data, punitive fines, embarrassment and loss of customer confidence. That said, your organization’s security policy sets the tone for proper security practices that all employees and business partners abide by. If followed—and that is a key point—the policy helps mitigate security risk.

What should you keep in mind when developing security policies?

- **Enforceability** - Do not create a policy that you cannot or will not enforce. The IT and security teams need the support, tools and processes in place to monitor alignment to the policy.
- **Exceptions** - The saying goes that there are exceptions to every rule - thus there are likely exceptions to every policy. Create a policy exception process to review, approve, and monitor exceptions within your organization.
- **Policies and Standards** - Policies, by definition, are general and high-level statements. The specific details and controls necessary to satisfy a policy should be contained within security standards, resulting in less frequent policy updates.
- **Accessibility** - Your policies will not be successful if your employees never see them! Keep your policies in a location that is accessible to all employees and be sure to communicate changes and updates when they occur.

Employee adoption makes or breaks your policies. Your employees are the key to the success of security controls, and need to be educated and reminded of the importance of information security. Regular, recurring security awareness training is an essential part of any cyber security policy program. Security policies should be included in new employee training and in recurring awareness campaigns.

The role of executive management

Executive commitment is one of the most important factors to the success of a security program. Executives that understand and support security policy make well-informed and risk-based decisions. As an executive you should be engaged in, and supportive of, security policies and set the tone by example at the top. Talk about security in your meetings and town halls. Practice good security yourself. Employees will follow your lead. While executive commitment does not guarantee success, its absence can certainly increase the likelihood of failure.

Organizations should adopt security policies and integrate them into all of their business functions or risk immeasurable loss and consequences. Executives: be a security hero and role model. Set expectations for secure behavior, policy compliance and follow through with frequent and recurring communication. Your security policies can help prevent potentially disastrous consequences.
LEVERAGING SECURITY RESEARCH AS A BUSINESS STRENGTH

There are no guarantees in the safety, security, and resilience of technology. Even with airtight security teams, policies, processes, and tools operating at peak efficiency, there will always be newly discovered software vulnerabilities. Your organization simply can’t test for every scenario and predict everything that might happen, there will never be enough money or time. Security inevitably becomes a balancing act. If you’re too cavalier about it, you’re inviting disaster. On the flip-side, you can invest as much as possible in as many security audits as you can afford, but sooner or later you still have to ship product to stay in business.

It’s usually only a matter of time until a company receives word from a researcher somewhere that they’ve found a security flaw in your product, service, or website. This is an opportunity for you and your business to demonstrate your leadership and commitment to customer experience and care. It all comes down to how you respond to the research. It’s not unreasonable to have imperfections in your code, and oddly enough, it’s often easier for third parties to spot these issues. This could be for any number of reasons: they’re less immersed in the detail; they have different background experience or unique knowledge and skill sets; they identify a user scenario you did not foresee. Some flaws are found accidentally, as was the case with five year old Kristoffer Von Hassel, who wanted to play his father’s Xbox games.

However a researcher makes their discovery, it will likely lead to an awkward conversation, and you may feel defensive having poured resources and man hours into development. What happens next—specifically how your organization responds to this kind of feedback—will mark you as either a great company that responds to its imperfections in a healthy, productive way, or one that would rather put its customers and intellectual property at risk by denying the problem exists, or worse, by trying to take legal action against the researcher.

To distinguish your company as one that truly cares about its customers, leverage the research community to make your products the best they can be. Researchers are effectively providing you with advanced product testing, which not only helps you ensure you are not putting your customers at risk, it can also help you drive innovation and demonstrate agility and leadership to your customers, prospects, and the industry as a whole. Building security into your offerings provides a competitive advantage and helps you increase customer loyalty and satisfaction. In other words, you can flip the bad news of a vulnerability disclosure on its head and use it as an opportunity to get customer attention and show that you take their security seriously.
Building security into your offerings provides a competitive advantage and helps you increase customer loyalty and satisfaction.

And the opposite can be true too of course — if you ignore or even try to take action against a researcher who finds a vulnerability in your product, you might be seen as more keen to cover up an issue than actually fix the problem.

Below are some suggestions on how to work effectively with researchers. Being open to the security community and their feedback is a great first step; we recommend you build on this with internal processes to streamline your response and increase efficacy of communications. **This is a coordinated disclosure program.**

**Some questions to get you started:**

- Do you have a written policy on your website detailing how your organization’s position on working with researchers, as well as a description of how your company receives and processes security feedback?

- Do you have an email address where researchers can send you their vulnerability findings? We recommend having a PGP key or some kind of encryption in place so people can submit this sensitive information to you privately and securely.

- Once a researcher sends you vulnerability information, do you have an internal system in place that ensures the right people get this information, and are those people empowered to take action?

- Have you considered a bug bounty program?

As we mentioned in last week’s blog post, the key thing to remember is that you are a custodian of your customers’ data, not an owner. There are various levels of engagement an organization can have with the security community and you will need to find the right level to suit your resources and needs. Even as a bare minimum, positive interactions with the security community and vulnerability disclosures demonstrates that you care about your customers, and it reflects well on your organization as a whole.

You don’t have to re-invent the wheel here if you don’t have the internal resources to get all of the above steps up and running. There are a number of websites dedicated to helping your organization work with the security community, such as HackerOne and BugCrowd, where researchers can submit their findings safely.
WEATHERING THE STORM OF A SECURITY INCIDENT

Today is the last day of October, and while we’re marking the last day of Cyber Security Awareness month in the US and Europe, many are also celebrating Halloween. So I think it’s appropriate we close out this series by facing our fears; today we’re talking about what happens after we’ve been attacked. How do you respond to a crisis?

Why is this important?

The website datalossdb.org tracks reported data loss incidents around the world, currently at a rate of seven events every day. That means the odds are pretty high that at some point your organization will experience some kind of security incident. You can reduce those odds by understanding your risk and mitigating it where possible, but you can never make yourself completely invulnerable.

It’s critical to understand this and take appropriate steps now. The way you respond to a crisis can make or break your business, and being prepared is the first step towards continuity and consistency in your business.

How do you prepare?

1) Map the Terrain

The first stage is to understand the kind of incidents you could end up dealing with. For example, you could be breached by an attacker; or a bug could be discovered in your products or services that exposes your customers to risk; or a bug could be discovered in a third party service or software that you leverage, again exposing your customers to risk. These are just a few examples, and response to each may require different actions and stakeholders, so it’s important to understand what the major scenarios look like and how they would impact your business.

2) Understand the Legal Requirements

There is a great deal of regulation and legislation around the collection and storing of certain types of data. Similarly there are requirements around disclosure should this information be compromised in some way while in your care, and these vary from state to state. You need to know how these impact your business and what will be expected of you in various security scenarios.

3) Agree on a Plan

You need to build a plan for each of these scenarios, identifying the various activities that are required for each and establishing SLAs for delivery. Know the order of certain processes and how various activities create dependencies on each other. For example, what is the process for launching an investigation, at what point should law enforcement be notified, and how does an investigation impact your communication to customers and the community?

4) Determine Roles and Responsibilities

Part of building a plan is assigning roles and responsibilities for core stakeholders. It’s important everyone is clear on their role and the processes involved should an incident arise. It doesn’t hurt to practice – you don’t want the real thing to be the time you have to figure it out if you can avoid it.

5) Detection of Compromise

According to Mandiant, it takes an average of 229 days for organizations to discover they have been compromised. Frequently we hear of cases where organizations hear of their compromise through a third party such as the Secret Service or FBI. The longer it takes you to detect an incident, the worse the likely impact of it will be, so it’s worth investing in robust detection and response measures and staffing to cover them.
What Should Your Plan Cover?

Your plan should cover three main areas:
• Incident containment and mitigation
• Incident investigation
• Communication – both externally and internally

For each of these areas of activities, it’s important to break down the constituent parts and ask the following questions:
• Who owns the activity?
• Who are the other stakeholders, and what is the communication mechanism for managing the process?
• What is the SLA or timeline expected?
• Where does this fall in the overall process?
• What are the dependencies and threats?
• What are the legal requirements?

Effective Crisis Communications

In the event of a security incident, an organization will often have either a dedicated internal team, and/or seek external expertise for handling the technical aspects of the response, specifically containment and investigation. In many cases though, they will scramble to handle communications through their standard channels and personnel, who likely will not have a security background and will not be familiar with the terrain they find themselves in.

The team will be hustling to respond to a situation that will likely be unclear, with a lack of relevant experience, and frequently in the face of rumor, press interest, and panicking customers.

The team will be hustling to respond to a situation that will likely be unclear, with a lack of relevant experience, and frequently in the face of rumor, press interest, and panicking customers.

Effective Crisis Communications

In the event of a security incident, an organization will often have either a dedicated internal team, and/or seek external expertise for handling the technical aspects of the response, specifically containment and investigation. In many cases though, they will scramble to handle communications through their standard channels and personnel, who likely will not have a security background and will not be familiar with the terrain they find themselves in.

The team will be hustling to respond to a situation that will likely be unclear, with a lack of relevant experience, and frequently in the face of rumor, press interest, and panicking customers. In this environment, it’s easy to make a wrong move. We see organizations rush to get a statement out before they know the facts, or at the other end of the spectrum, fail to communicate at all. We see misinformation, confusing advice, avoiding and inconsistencies. This can turn an unfortunate situation into a reputation nightmare, and potentially increase the chance of lawsuits or other negative response.

So what’s the right way to do it?

Firstly, it’s important you consider INTERNAL and EXTERNAL communications as two separate, but highly co-dependent elements. Below are some critical “Dos” and “Don’ts” for managing crisis communications:

Internal Communications

• Do treat information as need-to-know during initial response. It’s tempting for those working on the response to talk about it, and it’s tempting for those not working on it to speculate. You need to create policies and communicate them clearly so stakeholders know what is expected of them and that information should be kept confidential.

• Do arm ALL your employees to handle inbound enquiries. The entire company should know who the approved spokespeople are (and you should have just one or two spokespersons to create greater consistency of message) and how they should handle inbound enquiries. There must be a clear escalation path.

• Do create an FAQ so employees can respond to customer and partner enquiries with consistent messaging. Even if you don’t want to give any information out, an FAQ can help employees anticipate questions and respond with grace and confidence, as well as providing consistency of message across the company.

• Do coordinate timing of internal and external communications:
  - Once you communicate to the company as a whole, the news will leak out, so you need to have an external statement ready to go out at the same time.
  - If the story has already appeared on social or traditional media, your employees will likely already be fielding questions and speculation, so again, you need your internal communications to coordinate with an external response.

• Communicating publicly before communicating with the internal team negatively impacts employee morale and creates confusion and speculation.

External Communications

• Do be responsive. Your customers will be in the dark and worried. Do what you can to help them understand what’s really happening and what they need to do to protect themselves. Communicate what you can as soon as you can, but don’t rush to do it at the sacrifice of clear, helpful communications.

• Do get your story straight. Be clear on who in your team owns message development, approvals, and delivery in advance. You will have questions coming at you from all angles, and the media may well
get involved, so take time to agree a clear message and try to anticipate various lines of enquiry so you are prepared with relevant, crisp responses.

- **Do keep it simple.** Focus on sharing information that will help protect your customers. Avoid jargon and unnecessary details that just create more confusion. If customers need to take action, provide simple, actionable guidance. If they don’t, state that directly.

- **Do live it, don’t just say it.** If there is an action you can take to protect your customers or help them protect themselves, do it and explain what you have done and why. Make it as easy for them as possible.

- **Do be transparent.** It’s very natural to be defensive in this situation and take an evasive approach. This doesn’t help your customers and it will likely bring more scrutiny your way.

- **Don’t over-share.** This is the other extreme of the point above. It’s important to be clear and to the point with your customers – tell them the information that is most meaningful for them. Do not share unnecessary or confusing information. And do NOT feed speculation. If you have an investigation underway, state that and share findings when you can. Do not provide theories before they are verified as fact.

- **Don’t let the media set your communications strategy.** Once the media starts to get interested in the story, you feel the pressure is really on. Do not allow this to trip you up. Communicate clearly that you are investigating and will issue a statement as soon as you have something to share. Having your message clearly stated in an internal FAQ will help you stay on point and avoid unnecessary confusion.

Written by Jen Ellis [@infosecjen] and Maria Varmazis [@mvarmazis] in October 2014.

Original blog postings:

- Security Matters to the Executive Team {Taking It to the C-Level and Beyond}
- Data Custodianship
- Coordinated Disclosure & Working with the Security Community
- Why Your Organization Needs Security Policies
- Crisis Response and Communication