# Cyber Security Defense Starts in the Office: A Tool Kit to Plan for, Uncover, and Remedy a Cyber Attack

Danielle Janitch and John Blanchard, Osborn Maledon PA

While most imagine the forces behind data breaches and cyber threats as diabolical Russian or North Korean actors, sitting in remote locations planning large scale criminal or state-sanctioned masterplans, the vast majority of breaches in the United States are caused *internally*. In addition to watching for attacks from across our borders, we should also be focused on what is happening in the next cubicle. Employees—poorly trained and not aware of the risks, or disgruntled and looking for revenge, or departing and simply looking for a competitive edge—are the weakest link in your data security plan. An employee who anticipates being fired may decide to gather the employee-roster (social security numbers and all) and publish it on the web. Or, an employee who decides that she could make a lot more money if she simply did what she was doing for herself may gather your customer database (including order histories, contact information, and contract termination dates) as an easy target list and head-start. For this reason, organizations should make sure that their cyber security programs adequately focus internally.

Every problem requires a tool kit. This article will provide a few of the best tools for combatting the internal threat (and a few external threats as well).

## Tool Kit Item 1: Human Resources Management, Policies, and Agreements

The first step in minimizing the internal threat is to limit access to sensitive data. Boundaries should be placed on employees both during and after the term of employment. To the extent possible and reasonable, employees (and business partners as well) should have access (including physical access) to company data on a "need to know" basis. If someone does not use the company's financial information, for example, there is no reason to provide access to that information. Controlling the flow of information will reduce the risk of a data breach. All too often, we see organizations refuse to invest resources into building systems capable of limiting access, only to end up spending far more after a data breach because information was disclosed unnecessarily.

Internal agreements and policies are another key component to managing risk. Background checks should be done to detect those that present a higher risk for launching an insider attack. Employment agreements should emphasize the employee's duty to maintain company-confidences, as well as prohibit the use of confidential information. For example:

- Define what the Company views as "confidential." This can be broader (and should be broader) than company trade secrets. For example: protect customer purchasing histories, personnel information and/or customer contact information.

- Prohibit on use of confidential information for any unauthorized purpose and require employees return all company materials on termination. Make sure the employee understands what are unauthorized purposes, including providing concrete examples of the most common employee mistakes.

- Confirm the company's ownership of intellectual property created during the employee's employment (including intellectual property created by that employee).

Another strategy is the use of post-employment restrictions[1] designed to prohibit the employee's "use" of the information they acquired while employed. For example:

- Restricting, for a reasonable term and in a reasonable geographic scope, the employee from competing with the company.

- Prohibiting employee from soliciting former customers with whom he or she dealt (or soliciting company employees).

Employee handbooks should define what information is restricted and confirm that employees should not take any information (and return any information that they have) when their employment terminates. Handbook policies can set up exit interview procedures that are designed to remind employees of their obligations and confirm that they have returned all company data.

Further, during and after employment, it is important to watch behavior. Security experts note that happy employees are less likely to engage in data breaches. Watch for sudden changes, such as paying off debts, traveling more or just not keeping the same hours as normal at work. If someone is suddenly working odd hours, when others are not around, it is a good idea to find out why.

With these tools, an employer can take quick and affirmative actions in the event that it discovers that a former employee is inappropriately using information. Once it is discovered that an employee is inappropriately accessing customer data with unknown intentions, the company can file an emergency action in court seeking the immediate return of the data. Depending on the severity of the data breach, this process can proceed extremely quickly and effectively. For example, in the case of an employee theft of sensitive consumer information, there is a high likelihood that a court will enter an *ex parte* temporary restraining order that would require the defendant to deposit the data with the court within matter of days after filing the request. If there

[1] Restrictions on post-employment activities, such as non-competes and non-solicitation restrictions, are difficult to enforce in most jurisdictions, even if reasonable and appropriate (and flatly void in California, for example). Where enforced, these agreements must be reasonable and tied to the protection of legitimate business interests—protection of client relationships or trade secrets.

is a breach, post-employment restrictions and policies protecting company information will be important evidence in any effort to stop the breach. Agreements and handbook provisions provide the company and its employees with guidance and key tools to use if there is an internal breach. There is, however, no "one-size-fits-all" approach to employee agreements and policies. These restrictions are only enforceable to the extent necessary to protect legitimate business interests and courts and agencies (like the National Labor Relations Board) will scrutinize these provisions. Your legal counsel can work with you to prepare enforceable agreements and handbook provisions.

**Tool Kit Item 2: The Data Breach Response Plan and Ongoing Security Program**

By now, with the increased level of awareness around the cybersecurity threat, all organizations should either possess or be in the process of completing a data breach response plan. No matter how small or large your organization, it can affordably put into place a well-thought out and managed breach response plan and ongoing security program. There are numerous experts, including lawyers and security professionals, eager to sell their assistance in this process. And there are several free resources available from the federal government and non-profit organizations to assist in planning.

For example, the National Institute of Standards and Technology publishes free online SP 800-61, the Computer Security Incident Handling Guide. This document provides step-by-step direction on how to develop and maintain a comprehensive policy and plan for cybersecurity threats. Importantly, it recommends that organizations prepare generally to handle any type of incident and more specifically to handle the most common incident types. As discussed above, while the media focus lately has been on sophisticated attacks against the government and large banks and credit agencies, the most common incidents remain those against businesses with less than 1,000 employees that are due to mundane human failures, such as poor passwords, media or device security, or improper usage by current and former employees, contractors and vendors.

The Verizon Data Breach Investigation Report (DBIR), another free resource available online, should be regularly reviewed to stay informed of current trends, both in general as well as with your organization's industry. The 2017 Verizon DBIR, like all of the prior years' reports, found that the overwhelming majority (80% in 2017) of hacking-related breaches leveraged either stolen passwords and/or weak passwords. Further, one in four breaches involved internal actors engaging in unapproved or malicious use of organizational resources. Since 2014, the DBIR has identified insider and privilege misuse as one of the most common attack patterns. In 2017, 60% of such incidents involving insiders who absconded with data in hopes of converting it into cash in the future. The other top motivations for insider attacks identified in 2017 were unsanctioned snooping (17%) and taking data to a new employer or to start a rival company (15%).

So what is an organization to do? Do not wait for the breach to occur. Form a team now that includes members from throughout your organization (not just IT) and then leverage available resources to create (and regularly update) a comprehensive written plan that is tailored to the then-current threats that are most likely to impact your organization. Ensure that this written plan is given life within the organization through regular testing and employee training. Consider having each employee read and sign the plan annually, to emphasis its importance and prevent inadvertent mistakes by uninformed employees. Should your budget allow, engage experts to assist in this process where most appropriate for your organization. For some, this will be in the initial planning stages. For others, this may be in conducting penetration testing along with simulated-data breach events to identify gaps in your information security. For yet others, this may be in providing appropriate ongoing employee education.

It is important to make this investment in the preparation costs, as opposed to saving resources to focus on actual data breach costs. By being prepared, your organization not only mitigates the risk of an actual incident occurring, in the event of a breach, the organization's liability will be reduced due to its meeting or exceeding recommendations from regulators and industry best practices.

When a company has discovered a breach, it is important to act quickly. According to the Federal Trade Commission's guidelines, those steps should include:

- Securing your systems, stop the continued loss, and mobilize a breach response team immediately, including the consultation with experienced legal counsel.
- Fixing vulnerabilities with experts and create a comprehensive plan for dealing with the fallout from the public, customers, and employees.
- Notifying appropriate parties (which varies by law, state-to-state), including law enforcement.

The full guidelines from the FTC are helpful and can be found at https://www.ftc.gov/system/files/documents/plain-language/pdf-0154_data-breach-response-guide-for-business.pdf

**Tool Kit Item 3: Insurance**

Making sure your organization maintains appropriate insurance policies to protect it from all types of cybersecurity incidents is another important task. The first thing to keep in mind is that traditional forms of insurance typically do not cover cybersecurity threats. However, because the cybersecurity threat is relatively new to the insurance marketplace, procuring the necessary coverages is not as simple as one may presume. Unlike most other forms of insurance,

cyber liability insurance lacks standard forms and is not subject to industry regulation. Therefore, when comparing a policy from one company to another, price is but one factor to be considered.

Care should be taken to review the policy to make sure it includes the right coverages for your organization. Consider whether coverages include all types of cybersecurity incidents. For example, it is not uncommon for insider and privilege misuse incidents to be excluded from cyber liability policies, but available for coverage under employee dishonesty policies. However, the insured needs to make sure it purchases the right combination of insurance policies and riders to not leave itself uninsured for some or all insider and privilege misuse incidents.

Another concern is the scope of the insurance benefits. Does the policy cover investigation costs, notification costs, business interruption arising from hackers denying access to the organization's website or other assets (including how long the disruption must be before coverage kicks in), cyber extortion expenses, and/or personal liability (including libel) resulting from malicious use of the organization's website or other assets? Well thought-out cyber insurance policies should be tailored to individual risks for your organization, with coverages that map onto the most likely incident risk scenarios identified in the organization's data breach response plan and ongoing security program.

Don't forget the general exclusions. General exclusions can become unexpected pitfalls for the insured. Typical general exclusions, such as intellectual property, loss of personal device, third party bodily injury and bodily damage, war, terrorism, third party providers and negligence need to be carefully considered. For example, if your organization hosts its software through a third party cloud provider, you need to make sure the cyber insurance obtained covers incidents that may occur on such third party cloud provider's infrastructure, as well as loss of your intellectual property.

In addition to the general exclusions, there are two specific exclusions to keep in mind for cyber insurance policies. The first concerns the obligations that the insurance policy places on the insured to qualify for coverage. Because many cyber liability policies are modeled off professional indemnity policies, it is not uncommon for the policy to exclude any claims arising from facts or circumstances that the insured could reasonably have foreseen at policy inception. Insurance companies rely upon this exclusion to argue that, because the organization did not adopt certain minimum technology security requirements, coverage is not warranted. More recent policies may even expressly list required minimum technology security requirements. Care should be taken to thoroughly review any such requirements and document your organizations obligations to be in full compliance with them.

A second specific exclusion to watch for is the exclusion of claims occurring, in whole or part, before a specific retroactive date. Typically, insurance companies will attempt to set this retroactive date to the date the policy is purchased. But, because cyber security incidents often go months or years undetected, an insured is well served to ask that the retroactive date be as far

prior to the date the policy is purchased as possible. This is something that can frequently be negotiated, sometimes for an additional cost. If you are able to secure an earlier retroactive date, be careful to consider the interplay of this date with any minimum technology security requirements or general exclusion for reasonably foreseeable circumstances exclusions within the same policy. It would be a shame to obtain a favorable retroactive date only to be denied coverage under that exclusion.

In summary, insuring your organization against cyber security threats is not simple. It should be done only after the organization has conducted a thorough analysis of its risks and identified the areas where coverage is most likely to be needed. Further, once coverage is obtained, it should not be forgotten. Regular review should be an aspect of the organization's security program, done in conjunction with the organization's ongoing testing and review of its data breach response plan and security program.

**Conclusion**

While ransomware, malware, and outsider hacking are real threats to all organizations, care must be taken to not forget about insider attacks. The number of insider attacks compared to the other forms of cyber security threats may be lower, but the success rate and resulting damage from insider attacks is statistically significantly higher than any other form of attack. So, don't forget about them! Do background checks, watch employee behavior, limit sensitive information, control access, monitor, educate and make everyone of your employees active members of the organization's security program. Finally, because no amount of prevention can stop all bad actors, be ready with a well thought out and regularly reviewed data breach response plan and appropriate insurance. Every organization will face an insider breach. It is better to spend resources now to prevent and mitigate the damage when it happens to your organization, than spend (or lose in damages) ten or a hundred times more after the breach.