Threat From Within: Inside Counsel's Role In Defending Against Data Breaches

Insights
2.28.20

While organizations make significant investments in protecting their data from outside infiltration, they can often overlook the serious threats that exist within their own workforce. According to a 2020 study released by the Ponemon Institute, the biggest threat in terms of disclosure of sensitive information comes from so-called "insider threats," in the form of employees who disclose protected information or provide a means of access to that information to third parties, either unwittingly or otherwise. That threat has only grown in recent years, increasing by 47% in the last two years alone.

The Costs Can Be Staggering

According to the Ponemon report, each of these unintentional incidents can cost a company over $300,000. The average cost increases significantly – to nearly $900,000 – if an outside entity steals credentials from an unsuspecting employee and then misuses data. Incidents caused by criminal and malicious insiders can cost a company over $750,000 per incident, or over $4 million per year.

Depending on the situation, a company may incur costs for forensic surveillance, investigations, incident response, containment, and data analysis. The most significant consequences, however, may be the reputational harm, loss of goodwill, and loss of existing and prospective business as a result of a data breach. Some notable examples in recent years include:

- An attack on U.S.-based technology company AMSC, in which a former employee resigned but was able to copy and sell trade secret source code to a Chinese competitor company through continued access to AMSC's systems;
- A phishing attack on Sony Pictures Entertainment in which several Sony executives received phony Apple ID verification emails, which redirected them to phishing websites that accessed Apple ID usernames and passwords. Hackers used that information to access Sony's network, costing the company a reported $35 million in security enhancements; and
- An aggressive spear phishing attack directed at payroll employees across numerous industries, in which a spoofed email address appearing to originate from a company CEO or other senior executive requests payroll information that is then used to file fraudulent tax returns. This attack has impacted health care organizations, grocery store chains, manufacturing companies, educational institutions, financial services companies, and tech giants, to list a few examples among many.

Why The Recent Surge?

The most frequent cause of insider threat incidents is not the disgruntled or malicious employee. It is the employee who fails to safeguard data because of carelessness, negligence, or a simple lack of awareness of threats posed to the security of data that has been entrusted to the employee and the organization.

The increasing number of insider threats can be traced to many factors, including the common practice of permitting employees to have access to work email and company information on their personal electronic devices, sometimes without adequate protective measures to ensure the security of the data that resides on these devices. Another reason for the increase is the use of cloud-based applications to share company information with colleagues and to reduce the amount of data housed on the company network. And of course, trusting employees who fall victim to new and sophisticated strategies used by cybercriminals to access the company's systems will always be a cause for concern.

Company policies may require a series of preventive measures aimed at reducing risk. These can include requiring employees to have a password on all devices that are used to access company information; using a third-party, password-protected application for email access on employee phones and tablets; and using encryption software for exchanging confidential information.

Despite the fact that these policies have been in place at many companies for years, however, insider threats continue to skyrocket. These types of policies are not effective in reducing security threats unless (1) employees are properly trained to identify potential threats and (2) policies intended to secure sensitive data are implemented and consistently enforced across the organization.

First Steps: Awareness + Training

Protecting against insider threats begins with identifying sensitive information in the possession of the company and the employees who have access to that information. You should limit access to sensitive data to only those employees who need to access it, and you should retain the data no longer than necessary to achieve the purpose for which it was collected. You should consider implementing policies to reduce the risk of inadvertent disclosure of data, including requiring employees to use strong passwords that are changed regularly, installing necessary security updates, limiting the use of personal devices to access sensitive data, and reducing the risk of introducing malware to the company's systems by restricting access to outside websites.

Proper training is also critical to reducing the threat of disclosure of protected data. Once you have identified the employees within your organizations who have access to sensitive and protected information, you should ensure that those employees receive training that will enable them to identify and avoid potential threats. Those threats can come from many sources, including email phishing attacks, social engineering attacks, spear phishing attacks, hidden malware, and credential theft, among other things.

You should provide training to address and avoid these attacks in multiple forms and at regular intervals. This can include annual videos that may require employees to answer questions and achieve a passing score. Training can also include "phishing" attack drills created by the company to test employees to ensure that they can identify malicious emails and they know to avoid clicking on links that may contain malware.

One practice is for companies to utilize test spoofing emails, such as an email that appears to be sent by a colleague but where that colleague's email address has been changed by one letter. The email might ask the employee to click on a link. An unsuspecting employee may not be paying close attention, believing they are receiving an email from a colleague, and take a step that could one day lead to danger. This type of test can reveal which employees will need more dedicated training.

Advanced Tactics

Another procedure that you can implement to reduce the risk of insider threats is to require multiple forms of authentication or requests of certain sensitive information. You can identify specific individuals who need to confirm certain requests and require employees to use contact information provided by the company in advance, rather than any contact information provided in a potential phishing email, to ensure the validity of the request.

Insider threats posed by malicious employees seeking to harm the company pose yet another threat. Recently, in 2019, an employee of Capital One's cloud hosting company accessed more than 100 million Capital One customer accounts and credit card applications, which is expected to cost the company up to $150 million in breach-related expenses. You can guard against this type of threat through preparation of procedures designed to identify employees who are most likely to pose a threat and prevent them from accessing sensitive information.

This could include policies that immediately disable employee access to company systems once an employee has resigned or been terminated and require collection of company devices and equipment through which sensitive information could be accessed at the same time. Additionally, by limiting employees' ability to upload or download sensitive information, either through an external device or a cloud-based service, you can make it more difficult for a disgruntled or otherwise malicious employee to export sensitive data. Careful monitoring of work email can also help to guard against this type of attack.

Conclusion

Threats from within the organization continue to be on the rise and you should take the necessary steps to ensure that policies are being consistently enforced and employees are being properly trained on safeguarding company information. By taking the necessary steps, you can reduce the likelihood of confidential data exposure and the associated costs.

Risa B. Boerner is in the Philadelphia office of Fisher Phillips and is Chair of the firm's Privacy and Cyber Practice Group. She can be reached at rboerner@fisherphillips.com. Jeffrey M. Csercsevits is

Of Counsel in the Philadelphia office of Fisher Phillips and is a member of the firm's Privacy and Cyber Practice Group. He can be reached at jcsercsevits@fisherphillips.com.

Related People

Risa B. Boerner, CIPP/US, CIPM
Partner
610.230.2132
Email

Jeffrey M. Csercsevits
Partner
610.230.2159
Email

Service Focus

Privacy and Cyber