Cyber Threats:
Exposures and Breach Costs

Alliant

Issue No. 2

THREAT LANDSCAPE

Technological developments do not only enhance capabilities for legitimate business–they are also tools that may be utilized by those with malicious intent. Cyber-criminals include hackers, extortionists, identity thieves, and others of illegitimate purpose. These criminals actively seek out the vulnerabilities of business networks and systems and exploit such vulnerabilities, many for profit. Third-party threats are growing. Illegitimate exploitation of computer systems has become its own industry, where network attacks and security breaches are sold as a service.

Threats do not come exclusively from malicious outside sources. There are numerous internal hazards in each business. Rogue employees can use their access to company networks to steal and then sell private information; they can also create system vulnerabilities that outside parties can exploit. Another internal issue is technology error–there can be issues with program and service updates and upgrades; difficulty transitioning between software products; and technology vendor-side failures, glitches, or service alterations.

By far the most prevalent cyber issues, though, are the product of internal human error. Employees lose their network-enabled portable devices. Confidential information is accidentally sent out to improper recipients. In some cases, problems arise out of non-compliance with, or lack of notice and understanding of, company technology use policies.

Companies should be aware that while risk of exposure cannot be reduced to zero, there are ways to mitigate risk, starting with coming to know the threat landscape. Reducing the element of surprise when it comes to network security and privacy protection is the best way for a company to be prepared to mount an effective response to a breach.

EXPOSURE AVENUES: A BROAD, BUT NOT EXHAUSTIVE, LIST OF RISK PATHS

PHYSICAL LOSS

Even in the digital age, physical losses of company materials are not an uncommon source of risk. Sensitive data is still sometimes stored on paper, and even when it is not, there are tangible devices supporting intangible information that are susceptible to loss and theft. When thinking of device loss and theft, people are more likely to think first of laptops, smart phones, USB drives, and now tablet computers–and this is not a bad thing. Those devices are the most likely to go missing with protected private information stored on them or accessible by them.

It is critical that companies not forget, though, that other digital devices hold sensitive data and need to be included in protective policies. Desktop computers, printers, and copy machines may be more difficult for a novice criminal to steal because of their physical size, but are more likely to be rented devices that can be points of exposure if returned by a company without their data being properly cleared away. This can apply to office phones and card readers as well. These types of loss are not the most technologically sophisticated exposures today, but continue to be among the most common.

NETWORK VIOLATION

Network violation in the most general sense is using unauthorized access to data to alter or disclose that data in ways that are prohibited by the company, and often also by law. Illicit use, manipulation, alteration, deletion, or other destruction of data is obviously something that any company would want to avoid, and is therefore something that needs to be anticipated and prepared for. These threats are the reason critical information is often backed up on multiple, unconnected devices. Alteration and loss of data are not the only ways in which the data may be used in a manner contrary to company policies and goals. Improper disclosure of protected private information, whether it is contractually protected confidential corporate information or legally protected personally identifiable information, comes with huge legal and reputational consequences.

NETWORK EXPLOITATION

In other cases, it is the network system, as opposed to specific data, that can be used against a company. Malware and viruses can get into a system in numerous ways, both intentional and incidental, and are not only a problem for a company to address internally. Malicious code can move through a company's system to those of third parties, which may have been the actual targets all along. Affected third parties may view the victim company as the source of the malicious code, or at least view them as primarily responsible for the transmission of the code because their security measures were unsuccessful.

Another kind of exploitation of a network is when a malicious third party threatens a system for profit, demanding money or services in exchange for holding back cyber attacks or releasing captured data. One of the more common current variants of cyber extortion involves the use of ransomware, software illicitly introduced to a system that prevents legitimate users from accessing certain parts of the network and the data that lies within. The ransomware is removed, and access to the network locations restored, when the company acquiesces to the monetary or service demands of the extortionists.

SYSTEM INTERRUPTION

Systems and networks are not only vulnerable to misuse; they are also at risk of disablement. The most common means of network interruption are Denial of Service attacks, where a malicious third party orchestrates the overwhelming of a system with access requests, to the point where the system shuts down. While this kind of system-downing is most often seen as a direct malicious attack, it can also be the result of an excess of legitimate users attempting access simultaneously and unintentionally crashing the system. System and service interruption is not always the result of a Denial of Service event. Sometimes, a network will be disabled internally for maintenance, and these occasions can have complications requiring continued, unplanned network inoperability. This network inoperability is clearly an internal problem, but should be understood as a client-side problem as well for companies that offer any kind of or extent of access to their systems as a service to customers.

MEDIA AND COMMUNICATIONS MATERIALS ERRORS

There is exposure for companies when their information is misused; there is also exposure in cases where companies misuse information owned by third parties in their digital media. Communications over the Internet may include materials that constitute copyright or trademark infringement, and the inclusion of infringing materials can be easier to overlook when access to those materials is easy and ownership of materials is hard to confirm. This is a growing issue with regard to social media presence and the use of content created, and thus owned, by others in social media interactions.

SO THERE'S BEEN A BREACH: EVENT-RELATED COSTS AND ACTION IMPERATIVES

Cyber events demand rapid response, parts of which are often legally mandated and/or regulated. Companies do not have the option to downplay security breaches because of their contractual and regulatory obligations. The ensuing publicity of security failure means companies have further work to do in their responses as they seek to maintain the trust and confidence of their clients and the markets at large.

BREACH MANAGEMENT

Immediately after the discovery of a breach event, a company will begin to incur a number of expenses related to mitigating the impact of the breach. Forensic investigations must be paid for in order to determine the nature and scope of the breach. A public relations firm may be hired to try to steer public response and limit reputational harm. Legal consultation is required to determine the applicable breach notification laws, and then there are expenses to carry out any voluntary (as advised by breach coaches or PR consultants) or mandatory (as per federal, state, or foreign regulation) notification procedures. Notification costs include assessments of whom to notify, preparations and printing of notification materials, and mailings of such materials. Companies are frequently encouraged to purchase credit and/or identity theft monitoring for affected individuals to ensure quick response in the case of breach-resultant credit fraud or identity theft.

NETWORK RESTORATION

Other urgent expenses following a breach involve those incurred to restore the affected data and networks, and to restore their security provisions. In cases of credible threats to a network, or where parts of a network are held hostage by third parties, these costs are in the form of extortion payments and extortion-related expenses. In the case of network violation or exploitation, expenses are for the restoration of any data altered in the breach and the returning of systems and networks to a reasonably secure state.

CLAIMS EXPENSES

Security breaches often lead to class action suits from consumers and regulatory proceedings from governmental agencies. Defense in these cases can be long and expensive. Some companies choose to settle these claims, others are subject to fines and penalties. Of particular note are the penalties imposed under privacy-related legislation, and fines from the Payment Card Industry Security Standards Council.

BUSINESS INTERRUPTION

When a business is forced to disable its network, there is often loss associated with such action. The company is denied income it would otherwise have earned through payment card processing or online sales, and this lost income should be taken into account when calculating the financial damage a breach event has caused.

ANSWERING CYBER CHALLENGES

Businesses need to give serious thought to their computer systems/networks, and their web presence, and anticipate issues–faulty or illegitimate software and device vendors, changing data protection standards, and growing attack-as-service capabilities, among others. There is still constant probing and discovery at the outer limits of software capabilities as applications are adapted in varied and unexpected ways to enhance operations. While the reality of risk cannot be understated, it is also the case that there are several options for mitigating exposures and associated breach costs.

PREVENTATIVE THINKING

Technology best-practices are under constant development both within organizations and across industries and consumer bases. Putting in place necessary policies and protections is a key way for companies to limit exposure, and it can significantly cut down on the easiest and least sophisticated avenues of attack. Proper-use policies may also include internal education on risks, giving employees clear reasons for the rules they must follow, reinforcing the rules by increasing employee investment in compliance.

When it comes to more complex protections, there are several third party protective services that can be contracted to incorporate stronger security features into a company's networks. Information security companies' business is based around securing and protecting other organizations through implementation and maintenance of advanced firewalls, information packet monitoring, verification services, encrypted storage, and other network solutions.

VICTIM-PROOFING

Prevention measures are not fool-proof, and breaches do occur even when companies go out of their way to avoid exposure, so post-event recovery should also be part of risk management planning. Cyber liability insurance provides ways to recoup expenses in the aftermath of an event. There are provisions in cyber policies that address defense expenses, breach management, notification expenses and more, allowing a company to come out of a breach without massive losses of money or major blows to consumer confidence.

FOR MORE INFORMATION

For further information on the topic of this article, or on cyber exposures and cyber insurance, please feel free to contact Susanne Murray or Fred Podolsky of the Executive Risk Group of Alliant Insurance Services, Inc. The Executive Risk Group of Alliant specializes in all executive risk liability exposures and corresponding executive risk insurances, including directors and officers liability, cyber and privacy, employment practices, fiduciary, professional liability (errors and omissions), and fidelity insurance.

Susanne Murray
Executive Vice President
Executive Risk Group
smurray@alliant.com
212 895 0260

Fred Podolsky
Executive Vice President
Executive Risk Group
fpodolsky@alliant.com
212 895 0261