The MEARIE Group

The Reciprocal

Insurance, Financial & Business Solutions

November 2015

Cyber Extortion – An Important Cyber Risk to Understand

News of high profile cyber incidents, such as those involving Sony Pictures and more recently Ashley Madison this past summer, keep cyber risk in the headlines. Although sensational in nature (particularly based on the type of services Ashley Madison offers), this cyber incident provides some ideas on protection against these risks.

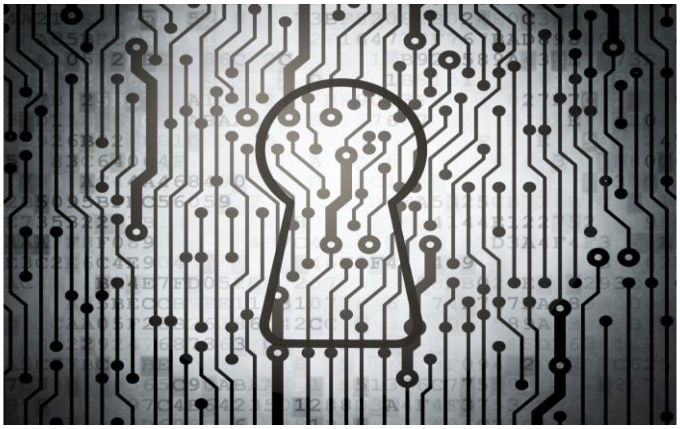
In this incident, data records of individual members were taken and then the perpetrators demanded the shutdown of the Ashley Madison website in return for not releasing the private data to the public. According to an article in Forbes magazine on this topic:

> "It was what is known as **hacktivist vigilantism**. The hacking group purposely targeted the Ashley Madison site because they felt the company profits "off the pain of others." Ashley Madison, no doubt, took a public approach to a semi-taboo subject (adultery) in American society, and arguably courted controversy as part of their marketing scheme. Unfortunately, no matter what your business is, there is probably someone that doesn't like what you do or represent (e.g. Oil companies, Planned Parenthood clinics, Medical research facilities, Microsoft, Sony, defense contractors, all the way to innocuous companies whose management has taken a public stance that has angered others) and is willing to go to some lengths to embarrass or attempt to undermine or destroy your business."[i]

When Ashley Madison did not concede to the demands, the data was released onto certain dark web sites and, for those interested, the information could be found, to the detriment of Ashley Madison and their customers.

Cyber Extortion

This is a compelling example of a fast growing type of cyberattack known as "cyber extortion." Cyber extortion can be described as an attack where a hacker will "kidnap" data through encryption or lock down a system or certain servers, demanding a ransom or some other action to be taken. This can put an organization in a very vulnerable spot and may create a conflict as to how to negotiate the way to satisfying the hacker without compromising the business. The intention is to hold the company for ransom and extort payment. Unfortunately, payment does not necessarily solve the problem. Payment does not guarantee: 1) the extortionists will not come back with more demands, 2) the release of the system or data, or 3) that the underlying vulnerability that caused the breach in the first place will be addressed. Expert investigation done in cooperation with law enforcement will help to determine the weakness that allowed the attack to occur.



Learnings from the Ashley Madison Case

There are lessons to be learned from the Ashley Madison case and consider in your organization's environment:

- **Be wary if 'hacktivists' identify you as a target** - It's important for any business which could suffer from release of its customer's personal information and/or proprietary data remain wary of potential threats from groups who would prefer that the business not be in business or the organization be damaged.
- **Ensure secure data is *actually secure*** –Thorough checks of password vulnerabilities and provisions for network segmentation are needed throughout the network. Understand the only way to improve security is to identify system flaws. And then make a plan to address them.

- **Realize deleted data can be recovered** – Deleting data from a business computer may not mean the data is gone forever. Computers generally retain file information until it's written over. So, if you have promised your customer you've removed their data from your system, ensure that's actually the case.
- **Be aware of your employees' internet activities** – People who get hold of data like this can use it against your employees and blackmail them in ways that could hurt your business. It's critical to educate your employees about security practices in relation to corporate devices and email addresses. Be clear about what is expected, and educate your employees about the potential threats of going against those security guidelines.
- **Security isn't just about computers** – Although unpleasant to discuss, insider threat is something to consider as well and may reveal certain vulnerabilities to your organization.

Reducing Your Risk

To reduce the potential your company will be a victim of cyber extortion, consider these steps:

- Identify potential internal and external threats
- Monitor social media, public forums or chat sites and identify the potential for ill will directed toward your company
- Identify employees (current and past) who may want to target your operations
- Plan IT Systems Audits on a regular and pre-planned basis to monitor, identify, assess and address potential vulnerabilities. Considerations should include:
    - Current software patches
    - Network segmentation so an attack in one area will not impact others
    - Ensure access controls are in place to protect data
    - Ensure network logs collect enough detail over a long enough time period to allow historical evaluation
    - Have current and up-to-date network maps

If a cyber extortion incident occurs, take measures to ensure the problem is being solved, communications are being handled and the damage is contained.

Check out this article from the American Institute of CPAs for some great tips.[ii]

Types of Cyber Extortion Attacks

There are various forms of attack cyber extortionists have used. Each scenario causes a similar problem, however, may require a different sort of response from your organization. Here are a few possible forms of attack:

- Denial of service (DoS) where an attack is initiated from outside your network using thousands of zombie computers to bombard your network with simultaneous traffic, knocking it offline
- Infiltrating or hacking into your network and then encrypting data to prevent the network's use, disabling critical systems or blocking access to sites
- Redirection of a corporate website by altering settings and then holding the site owner hostage
- Posing as cybersecurity experts, offering to analyze an organization's system to identify weaknesses and repair them on a fee for service basis. But rather than repairing potential weaknesses, exploiting the access for other means

The MEARIE Liability policy with Endorsement #8 Privacy, Cyber and Network Security Liability includes coverage for certain Data Breach Expenses, including expenses to retain a third party computer forensics service to determine the scope of failure of network security, but does not cover any ransom demands.

It is better to plan ahead in developing a response plan to help mitigate the risk. Your plan will be similar to the crisis management section of your Business Continuity Plan and should include:

- Management Team – overall responsibility to manage/respond to the extortion event
- Communications strategy – who will be notified, with pre-defined steps to speed sharing of information, particularly considering public relations
- Designation of Personnel – empowered to make decisions
- Established working relationship with security partners and law enforcement to reduce slow response times

Ultimately, investing in risk management over the long-term, rather than a short-term cure may keep your systems running, while reducing your vulnerability to cyber extortion.

This Reciprocal Newsletter is an electronic publication intended for Subscribers of The MEARIE Group's Insurance programs. It is published on a periodic basis and intended for information purposes only. In the event of specific claims, incidents or legal actions against the Subscriber, coverage will be determined by MEARIE policy interpretation.

Resources:
Government of Canada – Public Safety Canada
http://www.getcybersafe.gc.ca/index-en.aspx

Hacked! What to do if your company’s website is breached -
https://www.cpa2biz.com/Content/media/PRODUCER_CONTENT/Newsletters/Articles_2015/CorpFin/hacked-what-to-do-if-website-breached.jsp

References:

Canadian Underwriter, http://www.canadianunderwriter.ca/news/nearly-three-quarters-of-businesses-experienced-at-least-one-hacking-incident-in-the-last-year-study/1003657782/

Security Week – Rise of cyber extortion, http://www.securityweek.com/rise-cyber-extortion

CSO Online - CSO provides news, analysis and research on security and risk management,
http://www.csoonline.com/article/2911094/data-protection/cyber-extortion-a-growth-industry.html

[i] http://www.forbes.com/sites/ericbasu/2015/10/26/cybersecurity-lessons-learned-from-the-ashley-madison-hack/
[ii] https://www.cpa2biz.com/Content/media/PRODUCER_CONTENT/Newsletters/Articles_2015/CorpFin/hacked-what-to-do-if-website-breached.jsp