Five Things Every Company Can Do to Fight Cyberattacks

By David L. Schwed, CIO and General Counsel, MASS Communications

INTRODUCTION

In 2014, the number of detected cyberattacks skyrocketed -- nearly doubling from 2013, with roughly 117,339 attacks occurring each day, according to the latest Global State of Information Security ®Survey by Price Waterhouse Coopers.

These breaches are also costing companies more. The annual average cost per company of successful cyberattacks increased to $20.8 million in financial services, $14.5 million in the technology sector, and $12.7 million in communications industries..

Security Breaches Now Outpace GDP, Growth in Mobile Phones

Price Waterhouse Coopers finds that global security incidents now outpace the growth of mobile phones and the Gross Domestic Product (GDP). Security breaches grew

48% from 2013 to 2014, while global smartphone users grew only

22% and the global GDP increased 21% during the same period.

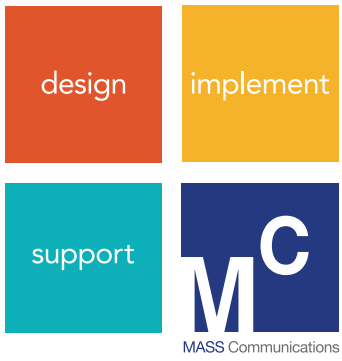
The growing use of mobile and cloud technologies have added more complexity to the IT threats to organizations. David Lacey, director of research at the Information Systems Security Association (ISSA-UK) said in Computer Weekly, "We are facing a data Tsunami with a 60% growth in mobile data. The threats are more sophisticated, data breaches more damaging, users have left the buildings and the applications have followed."

In response to the dramatic rise in security breaches, my firm, MASS Communications, a leader in IT connectivity solutions, works diligently with our clients to ensure security is a component when designing and implementing our solutions.

As MASS's Chief Information Officer and General Counsel, I'm leading MASS's new security service business. I already consult with our customers, advising them on how cyber criminals think and the ways in which they can better protect themselves from cyberattacks.

It's easy for leaders of small and midsized firms to look at the widespread networking breaches of the last few years and feel like there is nothing they can do. After all, if the likes of Lockheed Martin, Target, Citigroup, and the U.S. Department of Defense can't defend themselves against breaches, what chance does a smaller business have? Well, there are steps organizations of all sizes can take to minimize their risk. Remember, network breaches to Fortune 500 firms are certainly damaging to customer trust and the companies' bottom line, but in time, they can recover. However, a breach to a smaller organization's network can put the company out of business

The reality is there are steps you can take to safeguard your network beyond putting up a firewall, which by itself is inadequate in today's cyber threat environment. Below I offer simple things a company can do to begin to defend against cyber assaults.



1 Appoint an Information Security Champion

Too few companies today give information security a priority when evaluating vendors or making other operational decisions, and I believe they do this at their own peril. We're conditioned as IT leaders to focus on delivering the most value for the least money and overhead. Rather than looking for the lowest-cost vendor, we need to broaden our criteria and examine more deeply how these vendors approach security. "How can I (and my partners) best manage threats to my enterprise's IT environment?" should be the question we ask ourselves every day.

Security needs to be integrated within a company – it can't be an afterthought. The best way to begin is to identify and hire someone in your organization to serve as the company's information security expert. Most importantly, this expert needs a seat at the decision-making table when you are talking strategy and looking to grow your business.

2 Know your Data and Who has Access to it

A major step forward is to define your policies and procedures around information security – including devising a simple data classification system.

For example, a law firm may have different types of information – public, private, restricted, or highly classified. Each type of data needs information security controls depending on its sensitivity. If a law firm is working on a merger that only four partners know about, the firm needs to set up controls around that data, and only the people that have to have it, have it.

You can go a step further and track who is accessing the information using document management systems that require users to log in and check out documents, as opposed to relying on a file-sharing application that has no tracking capabilities.

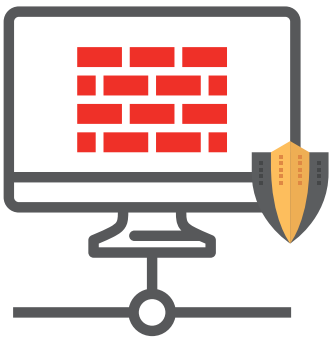
3 Do a Threat Assessment

Every organization should do a threat assessment, which starts with asking yourself, "Who am I trying to protect myself against?" Tied to this question is understanding what you have that someone else might want – it could be your product roadmaps, your strategic plan to expand into a new market, or a specific product. For example, in the case of Coca-Cola, their most valuable asset is the recipe for their famous beverage. The most common threat movies are financial, espionage, and ideology.

Keep in mind that your firm may not be the ultimate target -- a cyber criminal may want to use your network to get to one of your customers. An example of that was when hackers compromised RSA Security, a maker of SecurID keyfob systems, to gain access to defense contractor networks at Lockheed Martin and L-3 Communications.

Once you identify potential threat sources, then you can begin to look at how they are most likely going to attack your network. An excellent starting point is to do a perimeter vulnerability scan, similar to having someone ensure the security of your home by walking around the outside and checking to see that all doors and windows are locked to minimize an intruder getting in. This service scans your public IP addresses to see which ports are open to traffic and which are not so organizations can take steps to close ports that are not supposed to be open to external traffic.

4 Use these Technology Tools



You may wonder, "What tools should I invest in to maximize my network's security?" There are several, which I outline below. Some of these have limitations, which I've noted. The best approach to information security is to invest in multiple tools that can give you layers of protection.

- **Firewalls** – A firewall at a basic level looks at traffic and decides which traffic can come into the network and which can go out of the network. A firewall has limitations, especially if you are not monitoring its effectiveness and periodically reviewing the rules for the traffic you allow in or out.
- **Intrusion Detection System (IDS) or an Intrusion Prevention System (IPS)** - These appliances sit on your network. The IDS will identify possible network anomalies or possible attacks. Intrusion Prevention, which are similar to IDS but will proactively block the traffic as opposed to simply reporting it for further analysis. Most companies have a mix of the two.
- **Data Loss Prevention (DLP)** – These appliances can also sit on your network or software can be installed on hosts. They are designed to prevent the exfiltration of sensitive data. This is where a data classification policy comes into play.
- **Network Access Control (NAC)** – These systems utilize a number of different methods to determine who/what can have access to certain network segments. An example might be for companies to restrict access to their wifi network and only allow access for visitors who register their devices and have up-to-date virus software.
- **Security analyst** – Banks and other firms often have a team of people inside the organization who pour over the network traffic patterns themselves. They are trained to look for anything unusual that they can investigate further. Small and mid-sized companies won't necessarily have resources for an in-house security analyst or threat detection surveillance team. MASS Communications and other technology firms can provide different levels of network monitoring, and in the case of MASS, a report that spells out what areas in your network are vulnerable.

5 Implement Security Awareness Training for Your Staff

Quick Survey to Assess Your Employees' Security Readiness

At your next company meeting, spend five minutes surveying your employees on their information security awareness. Ask them these four questions:

Do you know how to identify a phishing email?

What type of threat actors should our company be protecting ourselves from?

If you see someone walking the floor that you do not recognize, do you stop them and ask them what they are doing?

Do you email yourself files from work using gmail etc., to work from home? Do you use dropbox or googledrive to store company files?

*Source: ISACA, 2014 Advanced Persistent Threat Awareness Study Results, 2014, www.isaca.org/apt-wp. All rights reserved.

Security begins with employees - your most important line of defense.

Safeguarding your network begins with educating your employees on the ways that cyber threats can occur. A 2014 survey* by global IT association ISACA revealed 62% of organizations did not increase security training in 2014, despite 20% of enterprises reporting they have been hit by advanced persistent threats.

One tactic that every employee should know about is social engineering – that is, the person who talks his or her way into getting access to your network. This intruder may call your company after hours posing as a senior manager, demanding that the security guard log onto the network so he can access important documents. Another criminal might pose as a guest speaker arriving early to your company. After being escorted to a conference room, she will ask for network access so she can check her email. Another hacker might infiltrate your office posing as a member of the IT help desk, and request access to your PC to do a software update, which will require you to type in or provide him with your login credentials. Criminals trying to access your company's network may approach you over email posing as the head of your college alumni committee, having researched where you attended school on your LinkedIn profile.

Another way employees are targeted is through "spear phishing." A hacker can look on your LinkedIn profile and find out where you went to college, and send you an email posing as the head of your school's alumni association, telling you that you are being given an award.

You should always look twice at emails. If you go to a tradeshow and are given a USB key at a booth, be aware that this type of removable media poses a threat to your company network. It's a very common way cyber criminals use to introduce malicious code onto the network.

Common Cyberattack Methods – A Cheat Sheet

What are some of the most common ways a company's network is compromised? The tools are varied with new methods being devised all the time. Here are some of the most popular techniques:

- Web – fake sites, session hijacking
- Wireless unsecured hotspots
- Email – links, attachments
- Mobile devices
- Social networking – Facebook, LinkedIn
- Malware
- USB (removable media)
- Social Engineering

Conclusion

To conclude, all of us should keep security involved in every conversation. Companies are always going to be concerned with churn and profitability margins, but a security mindset is one of the best ways to ensure your company and your customers are safeguarded. In short, security should be ingrained in everything we do.

It's also important to realize that security changes. Someone who was a threat to you last year may not be this year, so you need to constantly reevaluate your own threat environment.

About the Author

David L. Schwed is a co-founder of MASS Communications, a leading connectivity and telecom management provider that offers a full suite of voice, data, risk management, and security solutions.

David serves as MASS's CIO and General Counsel, playing a key role in formulating the company's strategic direction, and is responsible for the oversight of all legal matters. He has more than 17 years of Information Technology, Information Security, and Risk Management experience. He has worked in the financial services sector at a senior level for BNY Mellon, Merrill Lynch, Salomon Smith Barney, and Citigroup. He has also served as an expert witness in a criminal case in the field of computer forensics.

David is a member of the New York Bar and graduated Magna Cum Laude from Hofstra University School of Law.

MASS Communications, a leading connectivity and telecom management provider, takes a consultative approach to deliver a full suite of voice, data, risk management and security solutions. Founded by engineering innovators, MASS designs custom networks with best-in-class carriers across an international footprint. The New York-based Competitive Local Exchange Carrier made the Inc. 500|5000 List for three years running, 2013 to 2015.