Cybersecurity: If not us, who?

By Michael Senkbeil, CISSP, CISA

The statistics are sobering. Sixty-one percent of businesses that were hacked last year have fewer than 1,000 employees, according to Verizon's 2017 Data Breach Investigations Report.[1] One-third of small and medium businesses suffered a ransomware infection in the past year, forcing one-fourth of them to cease operations, according to a study performed by Osterman Research.[2] The direct costs of a single breach are now averaging more than $36,000, according to a report in Security Magazine.[3]

Over the past decade, multiple trends continue to expand: massive increases in the amount of data businesses store and rely upon for daily operations, increased use of multiple cloud-based vendors that house company data, and steady increases in the number of cyberattacks and data breaches perpetrated against businesses and consumers alike.

Cybersecurity should clearly be an issue getting direct attention from upper management and owners of small businesses. No longer should cybersecurity be relegated to the domain of the network administrator or outsourced IT support firm. Cybersecurity must be treated as a business risk issue, just as safety risk is in operations and competitive risk is in sales.

In this article, we will survey key elements of a successful cybersecurity program, an organized business process that is intended to protect data, thereby protecting customers and, in turn, businesses themselves.

Defense in depth

The phrase "defense in depth" is meant as a mission statement to inform the development of a cybersecurity program. Layers of protection need to be established at every business if we are to succeed in preventing hacks of systems and employees. Don't forget that people are hackable, not just systems. Every business should have a technology policy, including within it a cybersecurity policy and an incident response plan. As part of an ongoing cybersecurity program, the technology policy should be reviewed in its entirety every year.

Let's review the defenses against threats that attack a business via email. Technical security measures can begin defending a network even outside the firewall. Filtering email for threats and viruses before it is allowed to get to a user's inbox is an effective first line of defense. The firewall itself can help detect threats in the email stream, as it passes into and out of the network. The desktop or laptop PC can be protected by signature- and behavior-based antivirus and anti-malware software, providing another layer of defense. Finally, a well-trained computer user is the last line of defense in preventing this threat from succeeding. If a malicious email makes it through all the other lines of defense, the user can ultimately disarm a threat by deleting an email after using basic verification of suspicious data requests or by identifying malicious links in an email.

3-2-1 backup

Data backups address business risks, including fire, weather, power outage, and physical computer system failures like hard drive crashes. They also are an important component in reducing cybersecurity risk. A long-recommended model for data backups has been "3-2-1," meaning three copies of data should be maintained in at least two locations, one of which should be off site from the production computer system. The modern method for achieving this backup model is having a second copy of production data on site with the main servers, then have an additional copy of data stored in an encrypted, cloud-based repository.

Now that there are three copies of company data, care must be taken to protect all three sets of data from attack. Many businesses suffering a ransomware attack have had their backup data also taken hostage if the backup systems are allowed to be visible to the main data network.

Investing in a good 3-2-1 data backup system can also reduce business risk beyond cybersecurity threats. The offsite data backups can in some cases be used as a disaster recovery solution, providing ability to run servers on cloud storage for short periods of time even during disasters that include total loss of a building.

Network health maintenance

The root cause of the Equifax hack of 2017 was determined to be a known vulnerability in software used by Equifax. Customers expect the businesses they entrust with data to take reasonable effort to protect that information. Reasonable effort, in my interpretation, would include running supported software and installing security updates as they are made available by vendors. The simple act of maintaining software that uses automated tools can reduce by hundreds the number of vulnerabilities on each computer in a network.

Authentication and password hygiene

Compromised username and password information was utilized in more than half of the hacking-based breaches noted in Verizon's 2017 Data Breach Investigations Report. Implementing multi-factor authentication (requiring a one-time password or code in addition to username and password credentials) massively decreases the possibility of hacking using stolen passwords. Though it's slightly less convenient to use a multi-factor authentication system, the increase in cybersecurity is significant, relative to the effort needed to deploy the technology.

Reusing passwords in multiple websites or systems is a bad habit that can be cured through use of a password "vault" application. Password-protected spreadsheets or lists are inadequate in keeping passwords safe. Most password vault applications provide automatic password generation, topping the randomness and security of even the most creative passwords people can create. Of course, it's critical that the password to open the vault is a good password that won't be forgotten.

Conclusion

It's time that businesses treat the data with which they have been entrusted as the customer's, and protect it accordingly. As consumers, many of us were justifiably upset when our data was breached during the Equifax hack of 2017. This example should serve as a catalyst for businesses to become proactive about cybersecurity preparedness. Prepare your defenses with depth, then update and test them frequently, because hackers are doing the same against you.

[1] "Verizon's 2017 Data Breach Investigations Report." verizonenterprise.com. 2017
[2] "IT Security at SMBs: 2017 Benchmarking Survey." ostermanresearch.com. 2017
[3] "The Costs and Risks of a Security Breach for Small Businesses," Marquez, Oscar. securitymagazine.com. July 26, 2016

Michael Senkbeil, CISSP, CISA, is a partner at Chortek LLP in Waukesha. Contact him at 262-522-8248 or msenkbeil@chortek.com.