Defend your business against cyberattacks with these seven security-savvy strategies

This year, cyberattacks are projected to cause $6 trillion in damage.

Even worse, the criminals behind these attacks are more relentless than ever and are increasing their attempts to steal data, destroy reputations — and unleash havoc on companies of all sizes.
Phishing continues to be the leading cause of attacks. In fact, 91 percent start with a phishing email. And human error remains a major threat, accounting for 23 percent of all data breaches.

So what can companies do to protect their data, intellectual property and reputation from the ongoing and ever-more-sophisticated attempts of cybercriminals? Here are seven practical steps advocated by Aimee Barricelli, Chief Information Security Officer at Webster Bank, that can help you tighten controls and strengthen security across your organization.

#1. Set up a security operations center

Because hackers today are super-intelligent and ultra-relentless, at the bare minimum every company needs the expertise of cyber professionals in their corner. Whether your company employs an internal staff of security analysts and engineers or outsources this function to a private firm, a security operations center can keep your company safe from cyberthreats by providing key services such as:

- 24/7 monitoring of your organization’s systems, including networks, servers, databases, applications and websites
- Identifying possible security incidents or accounts compromised
- Keeping up-to-date on the latest threats and using information to improve detection and defense
- Quickly responding to security issues to mitigate damage
- Leading recovery efforts in the event of a security breach

#2. Optimize security tools

The good news is there may be no need to duplicate efforts to protect your data, because in many cases your company can leverage existing cybersecurity tools you probably already have. In fact, cybersecurity tools are designed to work together to protect your online properties. For example:

- Email security software can help you filter emails from external senders and tag them with specific banners and colors that alert employees of anything suspicious and make them more cautious about opening or clicking links within a certain email

According to recent statistics:

- There’s a cyberattack every 39 SECONDS
- Ransomware attacks occur every 14 SECONDS
- This year, a typical data breach will cause $13 million worth of damage
- Approximately 34 user logins are stolen every SECOND
- Eighty-eight percent of hackers can infiltrate an organization in just 12 HOURS
• Microsoft Outlook offers different settings that can be activated to increase security. Beyond requiring strong passwords, it offers two-step authentication when login occurs from an unrecognized device as well as the ability to alert internal users when they send emails to external audiences that may contain sensitive information.

“Sometimes cyberattacks are immediate. But sometimes they occur over time as each successful attempt allows the cybercriminal to enter your systems through little cracks or windows that ultimately lead right to your front door.”

—Aimee Barricelli, Chief Information Security Officer, Webster Bank

#3. Budget for cybersecurity and update software

Outdated or homegrown software applications can threaten security, especially those that either cannot be updated with the latest security patches or cannot integrate easily with other applications. If these apps store data, that may be exposing your company to unnecessary risk.

That’s why cybersecurity is not a one-and-done effort. Updates to systems and software must be part of annual budgets to ensure your operation is protected from the latest and most sophisticated cyberattacks. Keep current with security patches and software updates, particularly for corporation-wide phone systems, payroll systems and HR software, all of which include lots of private data that can expose your company to a loss of trust among your employees or customers as well as possible fines for breaching privacy.

#4. Educate employees

Since awareness and education are key to the success of any cybersecurity efforts, company leaders must commit to ongoing training for employees and staff. For instance, offering monthly tips or weekly emails, lunch-and-learn webinars and ongoing testing on specific topics can all encourage the use of best practices and keep cybersecurity top-of-mind for everyone within your organization.

“Hackers gain strength and momentum by the number of successful infiltrations they are able to make.”

—Aimee Barricelli, Chief Information Security Officer, Webster Bank

#5. Step up awareness of external emails

External emails are the entry point where many cyberattacks begin. Because hackers know today’s employees are: 1) very busy; 2) often preoccupied with different concerns; and 3) likely multitasking, they constantly devise new scams and malicious attacks. These are often based on “hot buttons” as a way to trick employees when their guard is down to entice them to click.

Fortunately, there are email management tools that call attention to messages coming from external senders by setting up informational banners and alerts like: “Be careful with this email. The sender may be an imposter.” You can also increase efforts to test employees on the latest phishing scams and hacks and offer remedial training for those who fail.
Gotcha!

Here are some opportunistic topics cybercriminals use in subject lines to make unsuspecting recipients click without even thinking:

• Urgent blood drives and need for donors
• COVID-19-related health expenses/payments/reimbursements
• National/presidential elections
• Food drives for storm victims
• Employee benefits renewal (particularly in October or November)
• Opportunities to buy stock, if your company is merging
• Requests from boss
• Direct deposit and/or payroll
• Recent purchase

#6. Consider cyber insurance

Because it’s human nature to click, it is inevitable that cyberattacks are going to happen. Yet only 34 percent of U.S. companies have a stand-alone cyber insurance policy.

Cyber insurance can be essential in helping your company get back on its feet after a data breach or ransomware attack because it can offer coverage for business interruption and loss of revenue, as well as reimbursement for investigative/legal costs or public relations services needed to help you restore your reputation . . . the sum total of which could approach thousands of dollars.

#7. Consult your banker

They can review your accounts and processes to make sure you’re using the latest controls, best practices and tools that can help alert you to potential cyberattacks and mitigate the impact. Tools like Web-Link® from Webster Bank provides a robust fraud prevention platform that can protect cash management functions, including payables and receivables, with advanced security technology, such as:

• Three-point sign-in and user login authentication
• Customizable account access and approval with dual control
• Security software for devices that access Web-Link, including mobile. It compliments your anti-virus software you should have running on all devices
• Behavioral-based fraud detection technology to protect the security of high-risk ACH and wire transactions
• Security alerts for account access activities like password reset, updated contact information and unlocked users
• Optional alerts, including outgoing wire confirmation and ACH approvals and exceptions
• Out of Band Authentication is optional security that enables two separate networks to authenticate a user, for use during ACH, wire and internal account transfer entries and approvals. It sends a one-time code to users via text or automated phone call
What to do if a data breach or ransomware attack occurs at your company

Even though you and your security operations team may have taken necessary steps in advance to safeguard your data and processes, you must remain vigilant. Always pay attention to alerts from your notification and monitoring systems. If you receive one that indicates something has happened, immediately disconnect from the network and contact your internet security team.

To further mitigate damage, make sure these steps are included in the recovery process:

• Isolate the server(s) and any impacted machines or devices
• Confirm company backups of critical data have not been affected
• Pull sensitive files off network
• Take steps to begin shutting down all systems to further protect data
• Work with local and federal authorities to share information that would help identify perpetrators or criminal networks

Although your operation may be down for a few days following a cyberattack, with safeguards in place, at least your company wouldn’t have to pay to rebuild systems or restore data . . . saving you valuable time and money.

“Hackers are extremely intelligent. They prey on human nature.”

—Aimee Barricelli, Chief Information Security Officer, Webster Bank

To get more information on how to protect your organization from today’s cybersecurity threats, check out the tools, tips and other resources Webster Bank has assembled to help raise awareness and provide guidance for maintaining a secure environment:

• Essential kit from the Cybersecurity & Infrastructure Security Agency (CISA), the nation’s risk advisor
• Secure commercial banking client solutions available from Webster’s Cybersecurity Center
• 10-point checklist to specifically guard against ransomware attacks

By making sure your workflows and processes are secure, you’ll be able to rest a little easier knowing you’ve taken critical steps to keep cyber criminals away and protect the future of your company.

Need help protecting your company from cyber threats? Contact your Webster banker to find out more.