BLR®
Learn. Comply. Succeed.

BAD CYBERSECURITY, BIG CONSEQUENCES

EDUCATE EMPLOYEES TO SECURE YOUR INFRASTRUCTURE

Bad Cybersecurity, Big Consequences

Educate Employees to Secure Your Infrastructure

Organizations are constantly forced to choose among myriad competing interests, be they staffing concerns, compliance requirements, IT infrastructure and hardware upgrades, or training demands, among others. All these factors are competing for a larger chunk of a budget that may not always be flexible enough to accommodate their needs. As the business landscape continues to rapidly change, organizational leaders turn to technological solutions to help meet these new demands. This means that there is an increased need for cyber awareness for employees at all levels of the organization as more business areas share the same networked resources. Additionally, doing business today requires using third-party vendors. While cost-effective and efficient, installing third-party software on your networks or using a water delivery service, for example, adds another level of security concern. Increasingly, these types of services are giving hackers a clearer opportunity to access private data stored on company networks or physical access to improperly secured servers or network end points.

Remaining vigilant in the face of growing cybersecurity threats presents businesses with a deepening cause for concern. First, let’s take a closer look at the problem and then explore solutions to help keep cyberthreats from affecting your organization.

The Problem: It’s Not Going Away

It’s no secret that cybersecurity breaches are affecting large and small businesses alike. Panera Bread, Under Armor, PumpUp, and Lord and Taylor, among others, have all had their customers’ personally identifiable information stolen from their networks by hackers. In addition to these straightforward types of data breaches, most cybersecurity researchers agree that there will be an increase in other types of advanced cyberattacks, such as ransomware and cryptomining malware.

Ransomware is also a constant presence in cybersecurity news. Multiple high-profile ransomware attacks have rattled both private and public sector networks, with aerospace giant Boeing and the cities of Atlanta, Georgia, and Baltimore, Maryland, all being affected. The ransomware used in the attack on a Boeing production plant in North Charleston, South Carolina, was a variant of WannaCry, a worm that initially appeared in the wild in May 2017; it appears that Atlanta was hobbled by a strain of the SamSam ransomware, which first appeared in 2015 in targeted attacks of hospitals.

With these advanced threats becoming a growing concern through all sectors of the economy, from retail to critical infrastructure, what is driving cybercriminals to expand the scope of their attacks?

A Lack of Preparedness and Awareness

Despite these highly publicized, costly cyberattacks on organizations, the business landscape is hindered by a lack of cybersecurity preparedness and basic awareness. In its *2018 Cyber Readiness Report,* Hiscox Insurance examined how prepared businesses are to manage cyberthreats. Its study revealed that nearly three-quarters—a full 73%—of businesses face major shortcomings in cybersecurity readiness.

Other key findings of the report that surveyed more than 1,000 U.S. companies include:

- **Cyberthreat ranks as a top risk.** While many firms may lack adequate defenses, two-thirds of respondents (69%) rank the threat of a cyberattack alongside fraud as a top risk to their businesses.
- **Cybersecurity spending is on the rise.** Almost 60% of survey respondents believe their overall cybersecurity spending budget will increase by 5% or more. Among survey respondents in the United States, 10.6% of their IT budget is being devoted to cybersecurity.
- **Costs range up to $25 million.** Among the largest organizations (more than 1,000 employees), the average cost of cybercrime, aggregating all incidents over the past year, was $1.05 million. Some of these larger organizations faced even higher costs than the average of up to $25 million annually.

According to findings from B2B research firm Clutch, employees at all levels of an organization are probably unaware of the IT security threats their companies potentially face:

- Nearly one-half (46%) of entry-level employees don't know if their company has a cybersecurity policy.
- Sixty-three percent of employees surveyed said they don't know if the quantity of IT security threats their companies face will increase or decrease over the next year.
- Among entry-level employees, 87% said they don't know if the number of threats will shift in the next year.

The survey also found that employees are less likely to recognize IT services as the primary area of security vulnerability at their company. Instead, they cited theft of company property as the primary threat to company security, ahead of unauthorized information and e-mail phishing scams. This lack of awareness puts companies at risk for cybersecurity breaches.

So, what can you do to fight back?

The Solution: Fight Back with Policies and Training

To start, follow cybersecurity best practices:

- Stay on top of software updates, and patch regularly.
- Build cybersecurity training into new hire onboarding.
- Provide employees with additional cybersecurity training such as microlearning opportunities or brown-bag talks.
- Stress the importance of using strong passwords to protect critical infrastructure and data, and teach employees how to create them.
- Have clear lines of communication for employees or contractors to report potentially malicious activity.
- Keep separate backups of critical data, and implement a regular backup schedule.

While these practices may not completely prevent malware from getting into your operation's IT network or infrastructure, they will help minimize any impact of an attack.

To increase awareness of IT security issues among employees, experts recommend that all companies maintain a "top-down" cybersecurity policy, where awareness of cybersecurity issues should be driven by a company's executive leadership. When company leaders emphasize and communicate IT security throughout their organization, their employees are more aware and prepared for threats. Employees of companies with a clear cybersecurity policy also feel empowered and are more likely to:

- Feel prepared for a cybersecurity threat;
- Accurately survey the number of IT security threats their company will face; *and*
- Understand IT services as the primary security vulnerability for their company.

Additionally, increased communication and training on cybersecurity policies is needed to make them effective. The Hiscox report cited above noted that employee training works—of the organizations making an investment in cybersecurity efforts, 54% indicated that employee training helped reduce the number of hacks and other cybersecurity incidents.

Another option is to regularly test employees' cybersecurity readiness through exercises such as phishing experiments. There are now cybersecurity firms offering software solutions to help IT security leaders gain a better understanding of how employees will react to a simulated social engineering attack, such as phishing, or to another kind of cyberattack. These tools, such as Barracuda Network's PhishLine or KnowBe4's Security Awareness Training programs, provide fast, accurate analytics, allowing a security team to visualize where their organizational weaknesses are and continually refine employee training on cyberthreats.

Train Them First, Train Them Fast, and Think Outside the Box

One of the most effective ways companies can drive cybersecurity awareness is through proper training during new employee onboarding. Clearly communicating such training policies can narrow the IT security knowledge gap between entry- and higher-level employees, helping ensure organizations as a whole are more aware and better prepared for potential security issues.

Not all cybersecurity training has to be through e-mailed policy, in-depth online learning programs, or classroom sessions, though; there are less structured approaches. Some IT departments have taken to developing their own training videos to complement and reinforce a company's cybersecurity policy. While most people expect Hollywood quality in their entertainment choices, they are more forgiving for IT or security department-created videos if they are short (no more than 5 to 7 minutes) and to the point. Most employees are familiar with YouTube and are used to watching short videos on their phone or tablet. It's easier than ever to create a decent video on a security-related topic using a smartphone or the camera system on your desktop computer and some basic editing software.

On the other hand, there are now many effective training materials developed by third-party learning and development and/or cybersecurity companies. While some of these are more traditional long-form training programs (either classroom or online), some companies have adapted their materials to meet the changing needs of the organizations they serve. In particular, many of these training programs are built around microlearning opportunities.

Microlearning is a form of training where a single objective, key idea, or concept is presented in an easily digestible format that has a beginning, middle, and end that is not dependent on or does not rely on other content. Examples of a learning mode or modality for microlearning are:

- A brief face-to-face coaching session between a mentor and a student;
- An infographic on paper, a website, a poster, or a mobile device;
- A podcast; *or*
- A message on a mobile device.

Incorporating these into a regular companywide cyber hygiene program could be an effective adjunct to more in-depth cybersecurity training.

Employees can also be given the opportunity to attend so-called voluntary “lunchtime learnings” or “brown-bag trainings,” where they can eat their lunch in a training room, conference room, or boardroom and hear from an in-house or outside speaker on a variety of security topics. These 30- to 45-minute sessions should be timely and relevant and feature cutting-edge information on the issues employees are concerned about. This could include:

- Personal Internet and e-mail security;
- Workplace cybersecurity threats and best practices;
- Refresher training on workplace policies and procedures surrounding cybersecurity; *or*
- Protecting employees from social engineering or identity theft.

Some of these courses may require the expertise of a local subject matter expert (or your IT/cybersecurity department), and these short sessions can be filmed for later review by employees who didn’t attend but who are interested in the topics. Above all, it’s important for trainers to keep their cybersecurity-related sessions—in whatever live or recorded format they use—short, entertaining, and informative.

Increased Consequences for Lax Cybersecurity

The consequences facing companies for lax cybersecurity are more severe than ever. Currently, all 50 states have some sort of data breach law on the books, with steep penalties for those found in violation. Potentially more damaging is the European Union's General Data Protection Regulation (GDPR), which took effect on May 25, 2018, requiring any company storing the personal information of any E.U. citizen to comply or face potentially bankrupting fines.

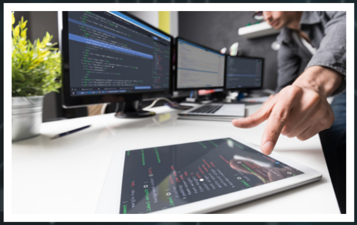
While expenses associated with training and cybersecurity may be a concern, the upfront costs are far cheaper than the fallout from an Atlanta-like cyberattack or a hack putting your organization out of compliance with a data breach regulation. In the end, your employees are your first line of defense against a cyberthreat. Making a small investment to keep them trained could be what saves your organization's reputation and keeps your doors open.

TrainingToday®

CYBER SECURITY TRAINING RESOURCES

From companies like Panera and Delta Airlines to government offices in major cities like Atlanta, Georgia, it seems no one is immune to cybercrime threats. What are you doing to safeguard your workplace against cyber security attacks?

TrainingToday® is here to help with our cyber security training resources:



The cyber security library will help you learn more about cybercrime and what you can do to protect yourself. From the different types of cyberthreats to e-mail security, this advice-rich library is a must for cyber security training.

Our microlearning: cyber security training is delivered in short, specific bursts at regular intervals throughout the year, aligned to the way your employees learn, and available via a mobile app or an online interface. If you're short on time but still need effective training, microlearning would be a great option.

Transform the way you train, and keep your organization safe with the help of TrainingToday.

BLR®
Learn. Comply. Succeed.

CONTACT US: 800-727-5257 | VISIT: HTTPS://INTERACTIVE.BLR.COM/CYBER-SECURITY-TRAINING-TODAY

a Simplify *Compliance* business

BLR®—Business & Legal Resources
100 Winners Circle, Suite 300
Brentwood, TN 37027
Phone: 800-727-5257
E-mail: *service@blr.com*
Website: *www.blr.com*