Oct 13, 2022

Categories:

Blogs
Technology Blog

Authors:

Gene F. Price
Matthew R. Schantz

You. Yes, You. Cybersecurity Awareness at the Company Level

The Department of Homeland Security (DHS) first declared October "Cybersecurity Awareness Month" almost 20 years ago. While many are still "unaware" of this auspicious event, it's important to understand why we still have it—even after two decades. Aren't we "cybersecurity aware" yet?

Well, no. FBI, DHS, and the Cybersecurity and Infrastructure Security Agency (CISA) each report that a lot of us just haven't quite taken in the message. Attacks of all kinds are still increasing, much of it because of lackluster cyber hygiene. We've all heard the great advice in CISA's cybersecurity basics for individuals, but while individuals serve on the front lines, businesses have what the threat actors are trying to get. So how do you make it less likely you'll be another victim and pay hundreds of thousands of dollars to get back to normal? FBT's Privacy and Data Security (PADS) Team has identified four actions a company can consider taking to bolster its cybersecurity:

Improve Your Cybersecurity Training

It's almost cliché that people are your key to success and profitability, but they are also your key to good cybersecurity. Work with your Human Resources group and your counsel to train employees every month—not just in October.

Use videos, interactive small groups, "phishing services," and the like to emphasize that it's OK to be suspicious of even friendly-looking emails. Cover common phishing techniques and other business email threats. Consider testing individuals with interactive media and explain the critical role of the company's MFA.

Expand your training to include vendors who have access to your network and insist they are trained at least to the same standards as your employees. Well-trained employees and vendors are your strongest defense against cyberattacks.

FBT Gibbons

Maintain Tailored Cybersecurity Policies & IRPs

Since every company has things criminals want, and every company is within reach of criminals around the world through their Internet connection, every company should know how to respond to an attack. “Cookie cutters” and templates are likely to be too much, too little, and simply wrong for the organization’s actual assets, business practices, priorities, and resources. Your policies should fit your organization.

Beyond policies to address individuals’ daily behavior, it’s critical that your organization have a good incident response plan (IRP) that outlines how the whole organization will respond when a cyber incident occurs. Company leaders should work with IT professionals and legal counsel to develop and regularly update an IRP so they can limit the fallout and get back up and running as soon as practical.

While an IRP lays out the backbone for any good incident response, if you quit after creating a shared document, your workers might freeze or run for the exits when a ransomware notice splashes across their screens. We recommend that your organization stress-test your IRP by routinely running “tabletop exercises” (TTXs). A TTX simulates an attack and tests how the IRP and your team react to specific cyberattack scenarios. We’ve never seen a TTX produce bad fruit, regardless of how poorly or well it was organized and run.

Since the company’s security depends on all individuals doing their part, include some non-IT, non-management personnel in those exercises. Seek and learn from their feedback, since their comments will reflect the challenges/potential contributions that many other team members can face/make to the effort.

Protect Your Sensitive Data

What’s sensitive data? It includes information that can identify someone, such as social security numbers, genetics, organization memberships, VINs, and much more. Both employees and clients generate tons of sensitive data that needs to be protected for the benefit of the business and the people attached to the business. Therefore, businesses must be proactive to prevent data breaches

and data exposure.

Sensitive data also relates to the company's "crown jewels" like finances and R&D. To prevent unauthorized access, take advantage of the helpful technology tools, including rolling out a password manager (to secure, keep track of, and update login information) for each employee, and maybe even a more advanced data loss prevention service to prevent copying or "exfiltration" of valuable information.

You may be asking yourself, "What's the big deal with protecting your business's data, and why would anyone want it?" Any type of unauthorized access to or use of your system is a problem. It could be a digital hack, where the hacker is looking for money by directly selling or using the data, or maybe a physical theft of information by a current employee. A breach could also involve a hacker lingering in your network, "listening in" for any data they may want to use in a way that will harm your business, whether or not they have a direct financial incentive to do so. Former employees might take advantage of their knowledge or continued access to cause you reputational harm. Protecting one of your greatest assets, your data, is key to maintaining your value and reputation.

Cultivate a Culture of Intentional Security

Users use computing devices, computing devices run on software, and software needs to be updated to fix vulnerabilities and bugs. Everyone in the enterprise should work in a rhythm that accommodates those updates, including regular restarts, patch installations, and after-hours staffing for emergencies and emergency communication systems.

Many security best practices rely on access partitioning, access limitations like "zero trust," and generally making it at least a little slower or harder to do the things that businesses are actually in the business of doing. Companies should set up their systems to monitor critical activities and to limit what individual employees can do and how systems interact so one mistake doesn't cascade into a catastrophic breach. And individuals need to understand how access limitations protect the company and keep it going.

FBT Gibbons

Good cyber hygiene takes consistent attention by any organization, but implementing these four priorities will help in that process. For help, please contact any member of Frost Brown Todd's Privacy & Data Security practice group.

FBT Gibbons