Fighting Cyber Crime: It's Not Just a Job for IT

Designed to access or destroy sensitive data, cyberattacks are an evolving danger to organizations. With millions of records stolen from data breaches every year, it's critical that your organization make cyber security a top priority—and this is not just a job for IT.

Employee users represent one of the most vulnerable links in the enterprise cyber security chain. Keep reading for tips on developing a cyber security strategy that will combat cyberattacks and empower staff to become cyber security experts.

63%

of attacks use compromised credentials

146

is the median days an attacker is undetected on a network

$500B

is the potential cost of global cyber crime

$3.8M

is the average cost of data breach

***Source:** Microsoft Threat Analytics*

Developing a Cyber Security Strategy

First, map out your threats and risks. Imagine what your worst-case scenario would look like. This could include theft of money (access to your bank accounts, wire fraud), exposure of data / personal identity information (student, donor, or employee records), availability of critical systems, theft of resources (for money), or ransomware.

Second, build out key controls. Now that you have a clear understanding of what you're trying to stop, lay out the controls that relate—combating phishing, protecting credentials, etc. Create initial controls against your top risks. For those that own or govern programs, leverage industry frameworks like the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF).

7 Key Focus Areas to Optimize Your Efforts

A balance of people, process, and technology.

1. **Know What You Have** – Keep an inventory of what assets you have and where they live.
2. **Manage It Well** – Keep your support contracts active. Apply patches when vendors release them.
3. **Manage Access (and multifactor authentication (MFA))** – Limit who has access to your systems (especially critical or sensitive platforms). If you are compromised or phished, limit the exposure.
4. **Manage Data** – Know where your data is and ensure you're comfortable with those systems' methods of protection. Utilize encryption at rest and in transit.
5. **Build the Right Visibility** – Now that you know where your data is, do you have logs and records of who logged in and accessed it? Collect the data and ensure it is reviewed regularly.
6. **Manage Your Vendors** – Where vendors store or access your data, ensure you are performing due diligence on their security program. Sample questions to consider: Do they adhere to their compliance requirements? Do they have a security program that you are comfortable with? Do they share third party audit reports (e.g. SOC2/SSAE16)?
7. **Empower Your Staff** – Develop a policy & require acceptance. Communicate it and provide basic education. If possible, invest in a security awareness program.

"Companies spend millions of dollars on firewalls and secure access devices...none of these measures address the weakest link in the security chain: the people."

—Kevin Mitnick, famous hacker

Building a More Vigilant Workforce

Make cyber security easy, fun, and approachable.

- **Create a Cyber Aware Program** – At minimum, have employees complete annual cyber security training but for best results, implement a year-round cyber security communications and education program. Create programs that educate employees about their role in protecting your institution but in a way that makes it easy to understand and remember. Hackers are constantly evolving their methods, so keep employees up to date on the latest cyber security news.
- **Build Awareness** – Start with a few core topics and communicate at an emotional level the impact each can have. Awareness topics shoul d be the same for home and work so that security becomes part of their DNA. Fewer topics are easier to reinforce and you should start with why people benefit. Example topics: phishing, password security, patching/updating, mobile devices, social media, and accidental data loss/exposure.
- **(Top Priority) Password Security** – The standard password is 10 characters but longer and more complex equals more secure. Avoid using personal information such as your anniversary or birth dates, pet's name, or home address.

Password Best Practices

- ✓ Enable multi-factor authentication (MFA) on any site you can
- ✓ Longer is stronger
- ✓ Avoid using personal information
- ✓ Use a passphrase
- ✓ NEVER share your password with anyone
- ✓ Use a password manager

Device Best Practices

- ✓ Set a strong device password or use biometrics
- ✓ Lock your device when you walk away
- ✓ Restart your computer at least weekly
- ✓ Allow it to make automatic updates

Watch the on-demand webinar, Fighting Cyber Crime: It's Not Just a Job for IT, featuring Blackbaud VP of Cyber Security, Rich Friedberg, and Cyber Security Communications & Education Specialist, Stephanie Pratt, to learn more about how you can start doing your part today. Plus, learn how Blackbaud is empowering its employees to become cyber security experts.

Watch now