Tools and Tech to Reduce Your Cybersecurity Risk

Vampire slayers have wooden stakes. Werewolf hunters rely on silver bullets. The Ghostbusters have their proton pack. This Halloween season, you may know the tricks of the trade for warding off spirits and ghouls, but what about cybercriminals and hackers?

Conveniently, October is also Cybersecurity Awareness Month. That makes it a perfect time to educate yourself about the tools and technologies compliance officers and information security professionals can employ to protect their organizations from cyber attacks.

Vulnerability Scans and Penetration Testing

Vulnerability scans and penetration testing tools are designed to head risks off at the pass. Vulnerability scanning software keeps a watchful eye out for weaknesses in your network, computers, and applications.

You may also consider engaging in penetration testing to put your systems under stress and see how they hold up. It’s better to uncover vulnerabilities in a simulation than leave them for a real hacker to unearth.

Virtual Private Networks

Virtual private networks (VPNs) have gained even greater relevance in our work from home/hybrid world. Internet connections in public places, like coffee shops or airport lounges, are not secure.

Anyone accessing your company’s information on an open network—be it through their work inbox or any SaaS service you use—leaves your system vulnerable to hackers.

VPNs create a secure barrier around your employees’ computers, keeping bad actors away from your secure information, even if they’re active on the same internet network as your team member.

Access Management

Who has access to what tools and information? And what level of access do they have?

Limiting access to sensitive information across your organization leaves fewer opportunities for malicious actors to gain access. Compliance professionals can work with the information security team to draw up guidelines around access levels for tools your organization relies on.

Similarly, revoking access should be part of offboarding employees and contractors. Ensure your team has a clear procedure for swiftly shutting down accounts when individuals leave your organization.

Device Management and Decommissioning

Access management doesn't just happen within individual tools and applications. The devices your team uses are equally relevant. Do you require employees to use company-provided devices, or is your organization BYOD? Perhaps you're in a hybrid situation.

No matter who owns the devices your employees use, it's crucial you have a say in how they protect them. VPNs, for example, are a simple way to protect PII no matter where or on what device employees access it.

Decommissioning devices should also be a part of your cybersecurity strategy. Do you have a plan for protecting data after a device has been retired? Your IT team should have a way to lock devices and wipe data in the event a device is lost, stolen, or otherwise decommissioned.

Customer Protection Methods

Just as important as securing information from your team's side of the equation is ensuring your customer-facing platforms are secure. Instituting multi-factor authentication, CAPTCHA tools, and single sign-on can reduce credential stuffing risks and keep clients safe.

Education is also key. Simply reminding your customers not to reuse passwords across accounts and to select passwords that are not easily guessed (no birthdays

or pets’ names) can make a significant positive difference.

Technology is the very thing that leaves you vulnerable to cyber attacks, but it can also be your silver bullet in preventing hackers and other fiends from accessing your valuable PII. Identifying the correct tools and tech is a team effort, but together you can create a secure web to protect data and information.