PUBLICATION

Cyber-Threats: Five Tips for Data Protection We Learned in 2017

Authors: Samuel Lanier Felker
December 15, 2017

Year-end is an excellent opportunity to reflect and get organized for the coming year. While making your list of New Year's resolutions, consider potential cyber and data security threats to you and your business and prepare for what we expect to be a tumultuous year filled with malware attacks, data security breaches and cybersecurity challenges.

To get you started, here is a recap of the top five tips we covered in our 2017 Cybersecurity Alert series, which addressed significant cyber-threats to your business and discussed ways you can protect your business with thoughtful and timely planning before an emergency arises. We offered guidance on establishing a smart data management plan, securing your company's portable devices, evaluating vendor relationships, handling disgruntled employees, and testing for data security events.

1. Plan Now for Data Security Events

As the number of data security breaches grows, it's not a matter of if your company will experience a security event, but when and to what degree. Is your company ready? Get your plan together.

- Identify potential security events. Know what data you have and where it's stored. Identify how access is granted, and to whom. Look for vulnerabilities in everything from your network to your employees' mobile devices to your company's website.
- Develop a two-part plan: prevention and reaction. Take steps to secure your platforms and data, and devise processes for remediation and notification in the event of a breach or other malicious attack.
- Review and test the plan. Document your data security policies and processes, and review them with your users, vendors and legal counsel. Continually test your information systems by simulating data security events.
- Revise and repeat. Data security plans should be continually reviewed, revised and updated – especially when technology is updated, a new category of data is retained or storage solutions change.

Read on: ***"Ready, Set, Go: Preparing and Testing for Data Security Events"***

2. Keep Only the Data You Need

Companies are continually building out their IT infrastructure with new applications, networks and platforms. As a result, they're amassing enormous volumes of data, making compliance with data privacy law and regulations more challenging than ever.

What's a company to do? Keep it simple by keeping only what you need.

- Know what types of data your company has. Identifying and managing data at a granular level helps you strike a balance between regulatory compliance and operational efficiency.
- Automate your information governance. Cloud-based solutions, in-place records management and AI can trim the fat from both your data storage and your data management processes.

- Get your data practices in line now because the EU's General Data Protection Regulation will be enforced beginning on May 25, 2018.

Read on: ***"Keep Only What You Need - Information Management in the Digital Age"***

3. Secure Your Company's Portable Devices

Don't assume your laptop or phone can't be compromised just because it's safely in your possession. Beyond the risk of physical theft, those devices can be hacked. Know these eight keys for protecting your portable devices.

- Make sure your data is encrypted, both upon transmittal and at rest. Most laptops, phones and other portable devices have some form of encryption built in – but if you're storing sensitive and confidential data, consider adopting more advanced options through a third-party encryption service.
- Require users to create complex passwords that must be changed frequently. Add further protection by adopting multi-factor authentication (MFA), which requires something in addition to a password, like a fingerprint, phone call or additional passcode generated from another source.
- Decide which users should have access to your data through portable devices, and which information they should be allowed to access. Create and monitor access logs to watch out for unauthorized access.
- Back up your devices and then secure those backups. Backups should be treated no differently than the original data; they should be encrypted and password protected.
- Remember to install updates and patches from the device manufacturers to stave off viruses, backdoors and malware. Inventory your devices regularly, and revoke from your network any that don't have the latest security updates.
- Use mobile device management (MDM) solutions, which offer a range of options, including allowing devices to be remotely controlled or wiped, setting minimum security requirements or requiring external drives to be password protected.
- Create written policies governing access to your company's data on portable devices. Clarify what's permitted and what's not. Disclaim liability for damage to employee-provided devices. Make clear that there's no right to privacy on devices that access a company's networks. Require users to execute an acknowledgment of the policies.

Read on: ***"Eight Keys to Securing Portable Devices"***

4. Vet Your Vendors Carefully

Vendors and third-party service providers that have access to your company's platforms and customer data pose unique security risks. Take steps to minimize risks when allowing access to your company's data.

- Before hiring a vendor, do a thorough review of its data security policies, procedures and controls.
- Be sure your vendor contracts provide for data security reporting standards, non-disclosure clauses, the right to require changes as the digital space evolves and a provision for your organization to have access to your vendors' systems.
- Even after a vendor is engaged, plan on continued oversight to ensure vendors are honoring their commitments and adhering to standards and processes outlined in your agreements.

Read on: ***"Vendor Relations – Your Best Friends Really Can Hurt You"***

5. Beware of Internal Threats

Disgruntled, financially-motivated or even careless employees can cause significant disruption and damage to your digital property. Employees know their way around your company's platform and data, and as such, have an advantage in launching malicious attacks against your information systems. Be on your guard for – and take steps to prevent – internal threats.

- Require non-disclosure agreements with new employees.
- Train your workforce to prevent unintended disclosure of confidential information.
- Protect devices and encrypt those that store your company's most sensitive data.
- Monitor user behavior and identify any unusual patterns.
- Manage access by regularly checking that user permissions are granted only for needed job responsibilities.
- Disable unnecessary accounts promptly.

Read on: ***"Disgruntled Employees and Other Internal Threats to Your Cybersecurity"***