A Henderson Brothers®, Inc. Whitepaper
March 2022

Corporate Safety Infrastructure & Protecting Your Business

The world of cyber insurance and cyber security continues to rapidly evolve. Cyber insurance had record rate increases in 2021 and there are no signs of slowing down during 2022. The types of attacks and vulnerabilities are changing quickly as bad actors are constantly testing and exploiting newfound weakness in corporate cyber defenses. The size and scope of ransom demands continues to increase exponentially. According to a Palo Alto Networks Unit 42 report, ransomware payments increased 82% from 2020 to 2021, or from $312K to $570K.

The Palo Alto report continues, there has been a rise in “quadruple extortion” ransomware cases. As many as four techniques are used in ransomware attacks: Encryption, Data Theft, Denial of Service, and Harassment. Ransomware gangs have started to use multiple techniques and more aggressive tactics when victims do not pay the ransom. Henderson Brothers expects the trajectory of attacks to continue to gain momentum throughout 2022. Smaller scale phishing-type attacks are also becoming much more sophisticated and prevalent. Due to these factors, carriers are continuing the require more stringent security controls and positions in order to offer coverage. Henderson Brothers has partnered with All Lines Security, a cyber security firm, to outline best practices that you can do to best protect your business from cyber threats and position yourselves to be best in class to the insurance carriers.

We know it can be daunting to begin to examine current cyber security protocols. Below we have outlined several key areas to focus on when you begin to think about your corporate safety infrastructure and protecting your business. This list is not exhaustive; however, it is a great place to start. Reach out to your Henderson Brothers team with any questions.

Secure your logins

- Employ Multi Factor Authentication (MFA) for all logins accessible from the internet, such as VPN, cloud email, and cloud applications.
- Employ Multi Factor Authentication (MFA) on your logins to internal privileged and administrative accounts, such as IT administrator logins to technologies such as hypervisors, remote desktop technologies, backup systems, routers, switches, firewalls, endpoints, servers, and authentication systems like Active Directory.
- Use strong, complex phrase-based passwords of 15+ characters in length.
- If you use Remote Desktop (RDP), make sure it isn’t accessible from outside of your corporate network through your firewalls. This is a primary attack vector for hackers.
- Practice using “least privilege” when giving access to users, i.e., only what they need to perform their duties. Successful hackers will have the same permissions as the compromised user.
- Employ secondary accounts for admins forcing everyone to logon to their workstation with a non-privileged account when performing common business functions, such as browsing the internet and reading email.
- Have too many passwords? Consider using a local password management solution to organize and protect logins to websites.

Backups are very important

- Backup all systems and data you need to operate.
- Regularly verify backups are occurring and are restorable (i.e., they are not corrupt).
- Utilize the 3-2-1 backup methodology to assure your backups are resilient to attacks and you are confident they will be there to restore business operations in a timely manner.

Train all employees on Cybersecurity and Ransomware

- Educate all employees using a security awareness training solution to provide regular and relevant training to your employees.
- Conduct phishing simulations (safe but real phishing attacks) so employees can put their training to the test and measure how much they’ve learned.
- Employees and their workstations are your first and most important line of defense against cyber threats. Make them your most effective part of your security team.

Plan and Practice Incident Response

- Maintain and practice a cybersecurity incident response plan.
- Maintain a disaster recovery and business continuity plan.
- Timely, effective, and efficient incident response can reduce damages and time your business operations are down.

Defend against Malware

- Deploy the latest endpoint security technologies to all workstations and servers to stop attacks. A Next Generation Anti-Malware and Endpoint Detection and Response solution from a well-known and reputable manufacturer is highly recommended. Endpoints, such as workstations and laptops, are the most common entry point for hackers.
- Employ URL and DNS filtering on endpoints and servers to ensure browsing is only permitted to approved, non-malicious websites.

Manage Technological Vulnerabilities

- Install security patches for all software and hardware to stop attackers from exploiting security flaws. Test patches quickly then deploy them each time they are available from the manufacturers.
- Frequent reporting of complete/incomplete patching is imperative to ensure all devices are properly updated. Use your software and hardware inventory to verify you’ve patched all assets.

Secure Email and Browsers

- Employ technology to protect from phishing emails, remove malicious attachments, and automate website checks. Many attacks start with a malicious email (e.g., Phishing).

Secure Mobile Devices

- Secure, manage, and monitor corporate-owned devices with a Mobile Device Management (MDM) solution. Device updates will be applied at regular intervals to ensure vulnerabilities are patched. Device security will be standardized to protect unauthorized access.
- If you permit personal devices (BYOD), secure company data using a Mobile Application Management (MAM) solution.

Protect Your Data

- Encrypt company information when stored and when transmitted, whether across the internal network or internet or on a server, workstation, mobile device, removable media, or in a database. Assuring that information is encrypted using accepted methods will hinder attackers from stealing it.
- Are you 100% certain where your sensitive information flows or is stored? If you aren't, then you cannot be confident it is protected. Create a logical diagram to show where it flows covering sensitive business information as well as regulated information, such as personal data, healthcare information, and payment card data.

Inventory your software and hardware often

- Take regular inventories of all hardware as well as software installed on workstations and servers, including operating systems. You can't secure technology if you don't know it exists in your organization. This inventory is important to verify all assets have protection.

Monitor security alerts

- Monitor all security technology alerts 24x7x365 so you can detect an attack and stop it before major damages occur. Building your own 24x7 Security Operations Center with a Security Information and Event Management (SIEM) technology is an expensive journey. If you don't have the budget, look to utilizing a Managed Detection and Response service to continuously watch over your business and guide you as threats evolve.

Hold your supply chain accountable for security

- If you utilize third parties for critical operations, assess your service providers to make certain they are securing your sensitive information as well as making certain their service is resilient to attacks. You need to know your information is safe in their care and the service will be there when you need it.

Segmentation is important

- Creating segmentation between different data sources, departments, divisions, and locations on your network will make sure attackers cannot easily traverse to sensitive or business critical areas. Whether it's from a user's workstation to critical systems, an effective segmentation plan will contain attackers and their damages when they strike.

Securely configure your technologies

- Make sure all technologies you use to operate your business are configured in a secure manner, including applications, workstations, servers, and network hardware such as routers, switches, and firewalls. Follow best practices from security organizations such as the Center for Internet Security (CIS) or the National Institute of Standards and Technology (NIST). Much like security patching, securely configuring your technologies will close security holes hackers would otherwise use to damage your business.

Cybersecurity firms can help

Consider using a cybersecurity firm to aid you in your journey to cost efficient and effective cybersecurity. Cybersecurity is a complex and evolving topic. Cybersecurity firms employ Chief Information Security Officers and highly skilled staff to help businesses develop, implement, and operate cybersecurity programs and all security technology needed. They can help you scale your program to the size and risk of your business as well as prioritizing the highest risk-reducing tasks first while maintaining cost and operational efficiencies.

Henderson Brothers' clients have access to cybersecurity experts through a partnership with the Cybersecurity Division of All Lines Technology ; experts that can help you solve your complex technology and cybersecurity problems and evaluate the best cybersecurity choices for your business.

Please contact cyberpractice@hb1893.com for further information.

You may also contact Seth Feldman at All Lines Technology at sfeldman@all-lines-tech.com.

Because you can’t expect what tomorrow may bring.
That’s why you have us.

Insurance • Employee Benefits • Financial Services

Our Mission | We will maintain our position as a respected leader in our industry by providing the best insurance protection, service and value for our customers.

Please note that the information contained in this whitepaper is designed to provide general awareness in regard to the subject matter covered. It is not provided as legal, medical, or tax advice, nor is it intended to address all concerns in your workplace or for public health. No representation is made as to the sufficiency for your specific company’s needs. This post should be reviewed by your legal counsel or tax consultant before use.

HENDERSON
BROTHERS®

920 Fort Duquesne Blvd.
Pittsburgh, PA 15222
hb1893.com