NORTHERN TRUST

YOUR GUIDE TO BUILDING AN EFFECTIVE CYBER SECURITY PROGRAM

A guide to Building an Effective Cyber Security Program

OFFICE SECURITY

Keeping company information secure involves physical and technical controls, including: physical security, perimeter controls, firewalls, patches and segmented networks. To read more about Office, Hardware and Software Security, *click the icon above*.

DATA SECURITY

Legal, regulatory and contractual agreements call for the protection of certain types of data, especially personally identifiable information (PII). Explore suggestions for improving the protection of your clients' data by *clicking the icon above*.

GOVERNANCE

Proper Cyber Security program management and sound data governance are critical to your company's long term success when it comes to the prevention, detection of and recovery from cyber events. *Click the icon above for more information*.

INDIVIDUALS / FAMILIES

Cyber Security risks are not limited to your office. The proliferation of mobile devices, online banking apps, social media and the "Internet of Things" have elevated the risk level to individuals and families. *Click the icon above for more information*.

OFFICE SECURITY

Despite the complexity of the current cyber threat environment, effective cyber security controls, along with education and awareness, will position your office in such a way as to reduce your exposure and negate many common threats. Experts agree on the key first step: start with the basics. Factor security controls into the decision making in every department of the business – such as accounting, information technology, personnel and family members. Use this step-by-step guide to assist you in building a comprehensive program for all areas of your office.

PERIMETER

- Restrict physical access to the office; keep access to servers and sensitive physical files to authorized personnel only.
- Consider installing CCTV cameras to monitor entrances, exits, servers and workstations.
- Inventory your technology assets: include servers, desktops, laptops, printers, mobile devices and removable media; use asset tags for identification and tracking.
- Store backup data in a separate location from your production network.

HARDWARE

- Remove unnecessary software from computers and laptops prior to distributing to employees.
- Regularly test your systems, applications and security controls.
- Block USB ports to prevent the exfiltration of data.

SOFTWARE

- Keep systems updated with the latest versions of operating systems whenever possible. Never use programs that are no longer supported by the manufacturer.
- Install patches in a timely fashion; if critical, consider midday installs and ensure users reboot as necessary.
- Use anti-virus software on all workstations (include scheduled scans as well as scanning of inbound files). Do not allow unauthorized software downloads, including internet add-ins.
- Install encryption software for data at rest and data in transit.
- Establish Virtual Private Networks (VPNs) for employee use to reduce the risk from working remotely.
- Utilize an email scanning program to examine inbound email and block spam and malicious messages.

DATA SECURITY

According to a study released by IBM Security in June of 2018, the average cost of a Data Breach per company is $3.86 million globally. This number, while alarming, is miniscule compared to the fines associated with the newly implemented General Data Protection Regulation ("GDPR") in Europe, where non-compliance can cost up to €20 million or 4% of annual global turnover (whichever is highest). Privacy and data security is high on the list of concerns for the public – which makes it all the more important for Family Offices to take proactive and aggressive steps to protect the data they have been entrusted to manage.

PRIVACY AND DATA SECURITY

- Ensure employees receive regular training on information security best practices, privacy principles and data protection requirements.
- Determine your regulatory responsibilities when developing your training program; different industries fall under the jurisdiction of different agencies. European companies or companies dealing with European data must follow the General Data Protection Regulation ("GDPR"), while US companies must comply with Gramm Leach Bliley Act ("GLBA") as well as Federal Financial Institutions Examination Council ("FFIEC").
- Implement a system of secondary approvers to reduce the risk of inadvertent errors. This may be something as simple as a "four-eye check" to proofread departing emails or something as comprehensive as a formal call-back process to verify financial transactions.
- Program pop-up reminders to notify employees when emails are going to external recipients and prompt for a specific acknowledgment of recipients before the message is released.
- Create and maintain a Records Retention program to manage the data you retain.
- Utilize a Data Loss Prevention tool to track the type and amount of information that is leaving your business.
- Use secure communication methods to send sensitive data to clients and customers, such as encryption. Encryption can be Transport Layer Security ("TLS"), which encrypts data on the move from one company to another, or a person-to-person encryption service such as PGP.
- Review employee access on a regular basis and implement technical controls to control who can view, edit, send and delete information.
- Avoid using "autofill" in email programs to reduce the risk of misdirected messages.
- Identify a classification structure for data and keep tighter controls around the handling of high risk information. For an introduction to data classification, check out "Every Executive Needs To Understand Data Classification Strategy" by Jason Milgram of *Forbes magazine*.

GOVERNANCE

A sound Information Security program begins and ends with governance; it includes policies, standards, procedures and training. Consider the following when building or refreshing your program:

- Establish a governing body to review and establish priorities when it comes to budget, projects and the strategic approach to Information Security.
- Conduct Information Security Awareness training for all employees. People represent one of the biggest vulnerabilities to your company – training must be comprehensive, engaging, and repeated with a frequency that reinforces the importance of following security best practices.
- Limit access to non-work related sites such as personal email, social networking, shopping and data sharing portals.
- Establish a process to build security and privacy tenets into projects from inception.
- Implement and prioritize secure coding protocols.
- Analyze the risk of third party vendors with a formal Third Party Risk Assessment program.
- Test and measure your control effectiveness.
- Have a cyber incident response plan and actively test the plan annually.
- Document procedures to follow if you suspect your business has been compromised.
  - Contact a company that specializes in post-breach forensic investigation for help with your investigation. It's a good idea to have an established relationship with one of these companies in advance for emergencies.
  - Understand when to notify law enforcement. If a compromise could result in harm to a person or business, you may need to notify local law enforcement quickly to report your situation and the potential risk for identity theft.
  - Consider hiring legal counsel with data security/privacy expertise, especially if you have client records that include PII. Counsel may also assist with engagement of forensic experts and law enforcement notification, as well as provide benefits of attorney-client privilege in certain situations.
- Hire and retain effective Information Security talent. Should you choose to outsource, perform extensive due diligence prior to signing contracts and define your Service Level Agreements ("SLAs") up front.
- Keep accurate records, logs, and audit results and apply the information gathered to consistently improve your program.

CYBER SECURITY FOR INDIVIDUALS

At its most fundamental level, personal cyber security for individuals and families must include three distinct elements: device security, sound security behaviors and physical (aka "perimeter") security.

DEVICE SECURITY

- Keep computers and mobile devices up-to-date with the most recent operating system, applications ("Apps") and programs. Whenever possible, program your devices to update at predetermined time.
- Use unique passwords. Consider the use of a password vault to allow for complex passwords that can be stored in a central location to avoid replication. Always change default passwords when setting up a new device.
- Secure your internet router with WPA/WPA2 encryption and change default passwords immediately upon setup. For detailed instructions on securing routers, review this resource from Consumer Reports.
- Use Anti-Virus software (usually available for free from your Internet Service Provider). Keep your virus definitions updated and schedule daily scans.
- Use a pin/passcode on your mobile devices and enable the auto lock feature. Experts agree that 5 minutes or less is a necessity.
- Understand the items in your house that may be connected to the internet and deactivate if not necessary. Common internet enabled objects include: televisions, security systems, thermostats, refrigerators, gaming systems, tablets, doorbells, wireless infant monitors, pet monitors and virtual assistant devices (Amazon Echo "Alexa", Google Home, Microsoft Cortana). Good or bad, the future will undoubtedly include an increasing dependence on internet connected devices, so a proactive approach is best (see "The Future of Internet of Things" in the *New York Times* for reference).
- For personal computers, use the settings feature to establish a minimum of two profiles. Your first profile/sign-in should be an administrative account. Then, create a separate account on the same computer with restrictions and enhanced security for web browsing. In the event of certain types of malware/ransomware infections, a separate login may allow you to access your files even if one section of your computer is infected. (Note: the malware will still need to be removed from the machine, but two or more profiles will increase the chance you will be able to access the settings to attempt to remediate the situation).

SOUND SECURITY BEHAVIORS

Sound security behaviors are essential for reducing the risk of falling victim to scams, fraud and cybercrime. Every individual needs to understand the safeguards that are required when browsing or conducting business online, as well as standard physical security precautions to prevent identity theft.

Understanding the risk for each demographic is essential. Older family members represent an appealing target for cyber-criminals, who are attracted to users with limited technical expertise but robust financial resources. Teens and preteens may engage in riskier behaviors such as file sharing, online game playing and multiple Social Networking accounts. Very young users are still learning how to navigate, and will need education regarding pop-up boxes and unwanted solicitation.

Each represents a unique set of challenges that must be overcome to manage the overall risk. Start with the checklist below to establish a suitable personal security profile.

- Review Terms and Conditions ("T&C") before agreeing to use Apps or websites. T&Cs allow you to understand who has access to your information and if they will share that data with others. Do not hesitate to avoid websites or applications that ask for information that is not relevant or necessary to the application's purpose.
- Understand privacy controls and keep settings as restricted as possible. Review privacy settings on a regular basis. In general, it is not recommended that you have open "social networking" sites of a personal nature.
- Do not overshare on Social Networking sites. Avoid posting information that indicates when you are or are not at home, where you may be traveling, or personal specifics such as your exact address or contact details. Be aware that social media "quizzes" and other popular "getting to know you" activities often reveal sensitive personal information, which may in fact allow cyber criminals to correctly answer security questions and gain access to accounts.
- Do not enter personal information or financial details into unprotected websites. Look for "https" instead of "http" and avoid unknown websites. Avoid shopping via Instagram, Facebook or personal blogs and instead go directly to websites.
- Do not save login details (aka "Remember Me" option) on shared devices or public computers.
- Use Two-Factor Authentication ("2FA"). Many of the most well-known websites have made 2FA readily available from the security settings of your online accounts, but it is up to you to turn on this free feature. This guide can help you turn 2FA on and help keep hackers out.
- Opt in for "paperless" statements. Electronic disclosures, statements and invoices eliminate the risk of lost or misdirected mail.
- Do not use public Wi-Fi networks to access any sensitive websites, particularly those that are related to financial activities. Even when protected with a password, using public Wi-Fi should be avoided for business or financial transactions.
- Keep a separate email account for your business, financial and health information to isolate from shopping, newsletters, notifications, etc. This should reduce the amount of "Phishing" and spam emails received on your important account.
- Learn to recognize and avoid Phishing emails. Phishing emails remain the top method for criminals to perpetrate fraud and infect computers and devices with malware. For tips, see "How to Recognize Phishing E-mails" on the Northern Trust Security Center.

- Clear browsing history and cookies on a regular basis. Although this may be different for each type of browser or operating system you have, general instructions can be found on both the Microsoft and Apple websites.
- If you must leave your laptop or a mobile device in your vehicle, keep out of sight and ensure your vehicle is locked.
- Keep your laptops and/or mobile devices with you in carry-on luggage while traveling.
- Alert credit card companies and your bank prior to traveling out of state/country.
- Follow best practices when using ATMs. Review "10 consumer tips for ATM safety and security" on Bankrate.com for easy-to-follow instructions.
- Keep track of your financial accounts, checking activity as often as possible. Question unrecognized charges immediately.
- Check your credit reports regularly. You do not need to pay for credit monitoring services to see a copy of your report; you can check www.annualcreditreport.com for details on how to obtain a copy of your report from each agency for free.
- Consider a credit monitoring account. Read "10 Best Identity Theft Protection for 2019" from www.consumersadvocate.org to obtain background on the leading companies.
- Do not share your home Wi-Fi passwords. It is recommended that you segregate your home network and create a guest network for visitors.

northerntrust.com Q62394 (4/19)