EARNEY & COMPANY L.L.P.
Certified Public Accountants

Cybersecurity Controls 101 : Keeping Your Systems, Data, and People Safe in 2021

Breaches of information security reported to the NC Department of Justice (NC DoJ) increased over 36% from 2019 to 2020. In North Carolina in 2019 there were over 8223 computer crimes *reported to the FBI* representing over $48.4MM in losses.

In March of 2020 alone, Barracuda Networks observed a 667% increase in phishing and malware Coronavirus themed attacks globally. In August of 2020, the NC DoJ reported to the Triangle Business Journal *that Privacy breaches related to ransomware in North Carolina had already increased over 100% from the prior year.*

Many small business ransomware cases go unreported for fear of privacy regulation fines and penalties, civil litigation, reputation damage, and breach remediation costs. Most of us know someone or even several individuals or businesses who have suffered an attack this year or last year. Small organizations are increasingly targeted due to low levels of protection in place.

Impacts of Ransomware and Data Breach:	Key Trends:
➢ **Data Loss –** crippling operations and relations / requiring rebuild at extensive cost ➢ **Operational Loss** – business interruption, lost customers / patients / clients / opportunities ➢ **Financial Loss** – breach remediation costs, civil litigation, privacy reg. fines and penalties ➢ **Reputation Damage** – lost confidence can sink the business. Ransomware is a $1.5 Trillion (*with a T.*.) criminal industry globally. It is important to ensure sufficient *preventive* controls are in place and that your information security and infrastructure enable resilience, most importantly your ability to roll back your systems and data to an uninfected state without significant interruption.	▪ Velocity and creativity of cyber-attacks are expected to continue in an exponential curve. Exploitation of legitimate software and attacks not detectable by antivirus / anti-malware applications will continue to increase. *Endpoint* Detection and Response (EDR) software that actively monitors, analyzes, and reports on abnormal machine and user behavior has become a critical control over the past year* *Endpoints are all devices connected to a network, such as laptops, desktops, mobile phones, tablets, and servers. ▪ Recent increases in the application of Machine Learning & Artificial Intelligence (ML / AI) by both hostile actors and network / endpoint traffic and behavior monitoring applications such as Security Incident Event Management (SIEM) and Endpoint Detection & Response (EDR). ▪ "XDR" comprehensive solutions will become more necessary and less cost prohibitive to small business. XDR provides threat detection and response across all layers of your network, email, endpoint behaviors, and cloud workloads by monitoring and analyzing traffic from all sources in a combined "data lake". XDR works together with SIEM and Endpoint Detection noted above.

EARNEY & COMPANY L.L.P.
Certified Public Accountants

Cybersecurity Controls 101 : Keeping Your Systems, Data, and People Safe in 2021

Critical Element	Controls (These are described further on pages 5-7)
1. Employee Education Over 75% of all successful cyber-attacks involve exploiting end-users (various sources). One compromised employee can take down a network…or an entire company.	✓ Cybersecurity Awareness Training / Automated Periodic Simulated Phishing Exercises ✓ Enforced Information Security Policy and Procedure / Acceptable Use Policy
2. Resilience Your ability to recover quickly in the event of an attack is critical. It is now "…a question of when", but the good news is that resilience is no longer cost prohibitive. Data and breach exposure can be limited.	✓ Data Backup Processes (that enable roll-back to a point in time) ✓ Network and Endpoint Protection / Logging / Event Reporting / ✓ Encryption of Data at Rest and in Motion (VPN for remote connections and Bitlocker for computer hard drives) ✓ Cyber Insurance (ensure includes ransomware)
3. Network Security Infrastructure & Access Controls The controls described right may look daunting, but they really are not. There are low-cost cloud-based solutions available to secure your network and configure your automated security policy settings. Several of these support Multi-Factor authentication and enable single-sign-on (SSO) for greater efficiency – even if you have mainly hosted (cloud based) applications.	✓ Advanced Firewall with VPN services for all Remote Connectivity ✓ Automated Group Security Policy Enforcement (enforce password complexity, change requirements, restrict local admin access, etc.) and Access Controls Based on Least Privilege ✓ Computer Operating System, Application, and Antivirus Updates, Spam Filtering ✓ Multi-Factor Authentication for the Network and Critical Applications
4. Threat Identification and Risk Management You can't fix what you can't see. These tools will enable your team to have visibility to enable capture and remediation of significant events or issues before they become a problem.	✓ Annual Information Security Risk Assessment and Security Planning ✓ Vendor and Cloud Provider Security Evaluation ✓ Security Incident Event Management (SIEM) Monitoring Software ✓ Endpoint Detection and Response (can enable system roll-back from Ransomware attack to undamaged state)

EARNEY & COMPANY L.L.P.
Certified Public Accountants

Cybersecurity Controls 101 : Keeping Your Systems, Data, and People Safe in 2021

The below are controls that will help keep your organization defended and resilient in the new threat environment. Whether you have an IT Managed Service Provider or in internal IT shop, we hope the below will help you facilitate a discussion on security priorities for your organization. If you have any questions, we are here to help.

Cybersecurity Awareness Training

One of the best defenses against ransomware, data loss, and business interruption is an aware and astute workforce. Automated cybersecurity awareness training coupled with simulated phishing emails, automated management reporting, and periodic scheduled short refresher videos are your best option. There are numerous products on the market at low cost ($2-$4 per user each month). Make sure you look at the reviews and have a qualified individual assess the quality of the education material and the simulated emails prior to committing to a package.

Group Security Policy and Access Controls

Have your IT team demonstrate to you how automated security policy is enforced via your Group Policy Object settings (GPO settings). GPO works with your Active Directory (AD) within your Domain Controller (DC- Server *or* Web based DC Services - for Cloud Networks) (AD- allows users permission to network resources and validates user credentials). In today's environment it is critical to have a secure network and security policies enforced by a Domain Controller. You can't just have a bunch of computers connected to the internet via a router with antivirus software. Whether you have ten users or a hundred, GPO and AD are needed to **enforce and monitor** important security policy settings such as:

Computer Operating System, Application, and Antivirus Updates

- Password / passphrase length and complexity, lockouts / reset requirements (every 90 days minimum…)
- Hard Disk Encryption (Data at rest - enable Bitlocker esp. on laptops) Password settings and hard disk encryption can help ensure a "Safe Harbor" defense in the event of a stolen machine with private customer or patient data stored on it. Your GPO settings, consistent new machine imaging (security setup), and sound hardware inventory processes are proof that security policy is applied consistently to machines.
- Disable local administrator access or restrict application downloads to keep employees from downloading malware inadvertently or changing local machine security settings
- Disable / restrict USB upload and download to prevent data loss or malicious file upload
- Verify users accessing applications (even online hosted applications) are valid current authorized network users (AD validation). Ensure that users accessing critical applications and network directories have the least access necessary to do their jobs, and enforce system segregation of duties.
- Enable internet content filtering / restrictions / secure DNS protection
- Manage operating system, application, and antivirus updates. Failure to deploy updates to your operating system and antivirus / antimalware can allow hostile

Cybersecurity Controls 101 : Keeping Your Systems, Data, and People Safe in 2021

actors to exploit *known* vulnerabilities *very* quickly. Have your IT team demonstrate to you how critical Operating System software such as Windows and antivirus / anti-malware updates are being pushed out to user machines regularly.

Encryption of Data at Rest and in Motion

For those using cloud-based network directory storage or file management, there are several hosted (online / cloud-based) solutions available now that are inexpensive and will enable you to ensure the devices connecting to your data and the people using those devices are legitimate, and that the machines connecting to hosted data are protected. These solutions can also facilitate Single Sign On (SSO – one password entry for the network and all applications, even hosted applications. An added benefit is that when you term a user account on the network, their access to all hosted applications is also severed).

It is important to consider user impact as you consider GPO automated security settings; there is a balance. User training and incorporation of user feedback is key with these implementations.

Multi-Factor Authentication

Critical network resources and applications should be protected by Multi-Factor Authentication (MFA), which requires you to not only enter a password but also prove you…are you (something you know plus something you have or have access to). In most cases this performed with a verification email address or the application may recommend an "authenticator" download for your computer or mobile device which requires you to enter a code to the computer from the auth app after you enter your password to log in. Fingerprint and face scans are common as well as a multi-factor option.

Firewall & VPN for Remote Connectivity

A Firewall is a minimum basic requirement for a secure network. While a secure router will identify bad traffic entering the network, an advanced firewall will stop it and alert you. Advanced firewalls offer logging trails and configured alert settings on traffic incidents, along with VPN support. Logging and alerting is important for ensuring a sufficient identification trail from incident to response and correction. This is especially important for organizations subject to rigorous privacy and breach reporting laws such as HIPAA, FERPA, and SEC Safeguard Rules.

VPN (Virtual Private Network) connections are the broadly accepted minimum standard for remotely connecting to your network. It is important especially now that organizations either discontinue use of Remote Desktop Protocol (RDP) or take additional steps to secure it. Most advanced firewalls come with built-in VPN capability and multi-factor authentication (MFA), providing a secure way for external users to access internal resources.

EARNEY & COMPANY L.L.P.
Certified Public Accountants

Cybersecurity Controls 101 : Keeping Your Systems, Data, and People Safe in 2021

Security Incident Event Management

Security Incident Event Management (SIEM) is a tool that will monitor firewall and network traffic and provide logging, reporting, and advisory on network events. SIEM provides IT security teams with alerts on potential intrusions for investigation. A staffed Security Operations Command Center (SOC) is often connected to SIEM solutions as an available service to provide real-time alerts to your IT team and recommended actions. This option can be more expensive. SIEM solutions can also be packaged with "automated SOC" or log analyzers (less expensive) which use "deep learning" to provide alerts and corrective actions to your IT Team.

In the past two years these solutions have become widely available at lower cost and are now regarded as accepted minimum practice for organizations with high data privacy and information breach ramifications. In the event of a successful attack, the SIEM logs and event detection capabilities are crucial in identifying the source and time of initial incursion / breach so that you know the exact date to "roll-back" your systems to secured point-in-time backup instances and avoid paying the ransom.

The bottom line is that corporate and nation-state hostile actors are now using artificial intelligence (AI)to exploit weak networks and the attack sequences are becoming more automated, thus the need for heightened use of AI / deep learning technology on the identification and response side. SIEM is critical for businesses processing confidential customer information, financial information, and providing trusted services (professional services firms).

Endpoint Detection and Response

Endpoint Detection and Response (EDR) solutions record and store behaviors on enterprise endpoints (mainly desktops, laptops, tablets & servers) analyze that data for suspicious behaviors and block malicious activity. Moreover, these solutions can provide contextual information on suspicious behavior and provide remediation suggestions.

EDR can help your enterprise detect cyber-attacks which slipped past your digital perimeter security (Firewall / Spam Filter / Anti-virus). Also, it offers granular visibility, threat investigations, and detection of *file-less malware* attacks (Equifax / DNC breaches 2019) by monitoring abnormal behavior in routine operating command frameworks (such as Windows PowerShell). Critically, it can provide security alerting prior to full compromise and enable roll-back to a secure system state in the event of a ransomware attack.

Spam Filtering

Spam filters are important to block unwanted emails soliciting products and services from entering your network inboxes. These messages can often carry phishing links or malware. Advanced filters often reside externally to your network and all email traffic to your networked computers routes through this gateway first before entering user inboxes. Advance filtering protection can include artificial intelligence monitoring of email content, protection from zero-day attacks, and 24/7 response teams that monitor and advise subscribers.

EARNEY & COMPANY L.L.P.
Certified Public Accountants

Cybersecurity Controls 101 : Keeping Your Systems, Data, and People Safe in 2021

Mobile Device Management

Mobile device management is an important control if your users are accessing network resources or highly confidential information (such as patient health information, trade secrets, or customer financial information) on portable devices (such as tablets / smartphones). A central administrator interface enables your IT team to track device locations, remote wipe data on those devices if stolen, enforce passcode security, and alert administrators to violations of security policy. Full "containerization" allows business data and applications to be encapsulated on BYOD devices and for private data / applications to remain private on those machines. The encapsulated data can be encrypted and have strict security policies applied to control information flow into and out of the device.

Backup Processes

A robust backup regimen is critical to ensure that your data can be backed up to a point in time. Daily incremental backups only keep your data as current as the last addition or deletion; there is no recovery capability for overwritten or deleted (or locked..) files. Understanding backup structure is important for your email applications as well. Choose backup regimes that provide secure separate backup instances for defined points in time. This will enable you to roll-back to a specific point in time to recover data (aka before the malware entered). This is critical in avoiding payment of ransoms and bouncing back from crypto-locked files. Several low-cost solutions are available that will provide Outlook backups as well as OneDrive. The backup reports should be reviewed daily, and backups should be test restored quarterly to ensure resilience.

Vendor Management & Cloud Security

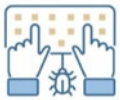
In several recent breach cases where the business or healthcare organization had a vendor breach, and the organization did not have an understanding of critical vendor controls (could not justify reliance), the courts and regulatory authorities have held the organization at fault. The assessed penalties and civil litigation costs have been high.

If you are utilizing a cloud based operating software application, or hosting data in the cloud, it is important to understand the vendor's controls over the security and recovery of your data. Most vendors processing or maintaining data, or providing Security as a Service (SaaS) should be able to provide you with a Service Organization Control report , known as a SOC 2 report, that details and describes an independent firm's (usually a CPA firm's) testing of these vendor controls. User control considerations are detailed in the back of these reports. They help you identify what vendor controls you can rely on – and what you can't. Make sure your vendor has sufficient support level agreements (SLA's) in place to ensure resiliency, and that their responsibility to notify you in the event of information breach is clearly stated in an executed service agreement or Business Associate Agreement.

EARNEY & COMPANY L.L.P.
Certified Public Accountants

Cybersecurity Controls 101 : Keeping Your Systems, Data, and People Safe in 2021

If you are using a Cloud IT Provider or a local IT Managed Service Provider (MSP), make sure they clarify in their service agreement with you exactly who is responsible for what related to security. Ask them to provide you with a copy of their Internal IT Security policy, and have them detail their monitoring processes and responsibilities over the controls listed here, as well as their service level agreements related to recovery times, breach notification and remediation. Find out if they and their co-location (cloud storage location) have their internal network security checked each year as part of annual "red-team" penetration testing. What are their service team members technical qualifications to monitor your security controls? You have a right to know.



Information Security & Acceptable Use Policy

Your key IT control processes such as provisioning and deprovisioning access, role based application access on least- privilege necessary, consistent security imaging of new machines, computer asset inventories, and secure disposal / destruction, along with incident management and disaster recovery processes and the aforementioned controls, should be documented in a brief but useful information security policy and procedure. Acceptable use of information assets should be defined as part of this policy, and it should be signed off on by all employees.

Information Security Risk Assessment and Security Planning

As significant changes are made to your computing infrastructure and critical vendors or service providers are added (annually for medium to large companies or companies subject to rigorous data privacy laws / high risk operations or data), a risk assessment should be performed to identify risks inherent to the specific environment, infrastructure, and applications, and the controls in place to mitigate those risks (Are the controls effective?). These assessments should be used to formulate the annual security plan which details planned new controls and any hardware / cloud-based infrastructure improvements.

Risk assessments are best performed by an independent assessor that has the technical qualifications and experience to effectively assess controls and potential exposures against the organization's risk appetite. Earney & Company has invested heavily in Technology Risk Advisory Services to serve our clients with an independent qualified lens on cybersecurity. Visit us today at www.earneynet.com.

Cyber Insurance

If your organization processes or stores customer personal information, personal health care information, legal, financial information, or provides trusted services, it is important to obtain cyber-insurance. The IT rider on your general liability policy will not cover breach penalties, civil liabilities, legal fees, PR team response, data recovery, or other breach remediation costs. A good cyber-policy will. Make sure that the policy explicitly covers ransomware. Read the fine print.

We hope you find this information useful and would look forward to helping as you evaluate your security infrastructure.