EARNEY & COMPANY LLP
Certified Public Accountants

Cyber Loss Prevention – Solutions for North Carolina Business in 2021 - 2022

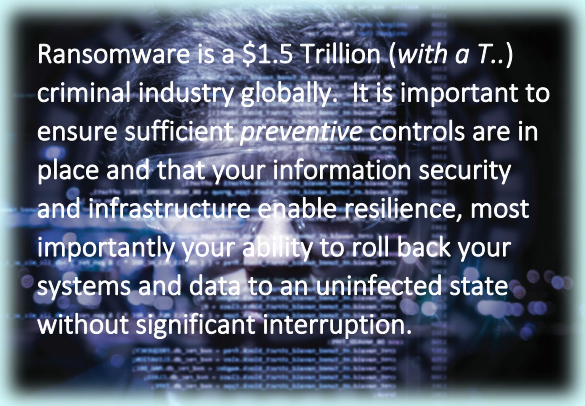
As of July 31, 2021, *reported* information security breaches to the North Carolina Department of Justice are trending to nearly double 2020's 1644 cases. The FBI IC3 Database received reports on over $27MM in victim losses from North Carolina business email compromise, ransomware, personal data breach, and phishing related activities in 2020.

In March of 2020 alone, Barracuda Networks observed a 667% increase in phishing and malware Coronavirus themed attacks globally. Nationally and statewide, we have observed attacks on cloud-based network and application providers adversely impacting businesses.

It is important to note that many small business ransomware and breach 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 or data loss this year or last year. Small organizations are increasingly victimized due to low levels of protection in place. Consider an *independent* cybersecurity risk assessment by a qualified professional to evaluate the effectiveness of your cyber and information security controls against the current threat environment.

Impacts of Ransomware and Data Breach:

- **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.



Key Trends:

- Velocity and creativity of cyber-attacks are expected to continue in an exponential curve. Exploitation of legitimate software and file-less 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.*
- 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).
- Extended Detection and Response "XDR" coupled Managed Detection and Response (24/7 incident support) are evolving as a necessary component for trusted service organizations and privacy regulated businesses. XDR provides threat detection and response across all layers of your network, including traffic, email, endpoint behaviors, and cloud workloads by monitoring and analyzing traffic and event logs from all sources in a combined "data lake".

For more information about Earney & Co. Technology Risk Advisory Services, please contact us at 910-256-9995 or at rduggan@earneynet.com Robert Duggan, CPA, CIA, CHC, CISA, CISSP

EARNEY & COMPANY LLP
Certified Public Accountants

Cyber Loss Prevention – Solutions for North Carolina Business in 2021 - 2022

Critical Element	Controls
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 with remedial education ✓ 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.	✓ Incident Response procedures coupled with tested and secure data backup processes which enable roll-back to a point in time and containment ✓ Encryption of data at rest and in motion (VPN for remote connections and Bitlocker for computer hard drives, volume encryption for privacy regulated servers) ✓ Cyber Insurance (ensure explicitly includes ransomware, breach remediation, legal, penalties)
3. Network Security Infrastructure & Access Controls The controls described right may look daunting, but they really are not. There are also 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, block USB port uploads and downloads, etc.) and access controls based on least privilege ✓ Automated operating system, application, and antimalware updates, spam filtering / advanced threat protection ✓ 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. *Consider a qualified independent assessment to evaluate cyber and information security control design effectiveness for your environment.* ✓ Vendor and cloud provider security evaluation / review of Service Organization Control (SOC) Audit reports ✓ Security incident event management (SIEM), extended detection and response (XDR), network (NDR) and endpoint detection and response (EDR) / logging / event reporting for trusted service businesses and privacy reg. impacted businesses

For more information about Earney & Co. Technology Risk Advisory Services, please contact us at 910-256-9995 or at rduggan@earneynet.com Robert Duggan, CPA, CIA, CHC, CISA, CISSP