INDACO RISK ADVISORS | BLUESTONE ANALYTICS

"Shelter/Safer in Place" mandates are forcing organizations to complete work from remote locations. In our attempt offer our perspective on best practices to protect information, we have connected with Liam Bowers, CEO of Bluestone Analytics, for his expertise and viewpoint.

Heightened Vulnerabilities

Phishing

- Known topics to gain entry:
  During this time when folks are on alert and seeking information, cybercriminals will prey on end user's desire to learn. There already are known phishing campaigns with — among others — the following themes:
  - Fake CDC links with global tracking maps, updates, etc.;
  - Charitable Contributions;
  - Airline Carrier Refunds; and
  - Fake Cures, Vaccines, and Testing Kits.

Remote Access

- Employees who are forced to work outside the office are potentially accessing sensitive information without the same security measures included in organization's internal perimeter defenses.
- System administrators accessing devices remotely to service employee needs, perform system updates, etc., may exposes those files.

> ***"A lot of companies were not ready for the transition to remote work and cyber criminals are definitely going to try to exploit that."***
>
> *Liam Bowers, Founder & CEO Bluestone*

Solutions

Employee Training

- One of the best ways to harden the defense of data is to improve your employees' knowledge and decrease susceptibility.
  - Educate the front lines on how best to avoid harmful content.
- Develop and revisit expectations related to personal devices, desktops, email, social networking, virus prevention, etc.

Network Connection

- Remote Desktop Protocol (RDP)
  - Companies rushing to implement RDP's in response to this working environment should make certain to implement two-factor authentication.
- Virtual Private Network (VPN)
  - A VPN provides internal-perimeter security protection to users anywhere in the world.
  - That means your company's security protocols are protecting your data vs. the firewall of an employee's local Internet provider or home wifi network.
  - Organizations should implement controls that force employees to sign into the VPN to help ensure data protection.

Company Perspectives

Indaco Risk Advisors

A concise set of security policies enables the IT team to manage the protection of information assets and maintain accountability. In addition to placing cyber liability insurance, these are topics we work with organizations to address during our risk analysis :

- Personal Device Use
  - Recognizing these devices can play a valuable role in convenience and productivity, what procedures can be implemented to protect data?
- Virus and Malicious Code
  - Implementing steps to protect your assets from destructive or malicious programs.
- Email Security
  - Outlining the types of "clickbait" to look for and defining expectations when a breach may have occurred.

Bluestone Analytics

Identifying and mitigating threats are at the forefront of protecting your business. We use advanced proprietary technology to proactively identify potentially volatile and costly situations and to quickly remediate cyber threats.

Remote Readiness Assessments and our Virtual Chief Information Security Officer quickly implement the controls needed to defend their data as unprecedented number of employees work from home.

- Cyber Incident Response
  - Our response process identifies the source of the incident and helps clients to quickly resolve the threat, minimizing impact to operations.

> ***"This is a great time to be proactive about cyber risk by implementing effective controls and emerging from this situation in a much stronger, more secure position."***
>
> *Liam Bowers, Founder & CEO Bluestone*