HORNE CYBER

CYBERSECURITY CONCERNS FOR EXECUTIVES & BOARDS

No organization is immune to the threat of security breaches. With cybercrime activity increasing rapidly, every organization needs to address potential risks to better protect its systems and sensitive data.

It is no longer "if" – but "when" – your organization will be victimized. The question every executive and board member will have to answer after that inevitable attack is "Did we do enough to protect our digital assets?"

The costs to a company can be staggering. Impact usually includes forensic investigation, time spent with law enforcement, crisis management, compliance requirements, credit monitoring, potential lawsuits, and damage to the company's brand and reputation.

Cybersecurity is not just an IT issue. Executives and boards should take a proactive approach and ask thoughtful questions to information technology and internal audit leaders. Below are eight areas in which you should pay particular attention.

1 Human Interaction

Human error and oversight are common causes of security breaches. If employees are not adequately trained, they can expose your organization to breaches by malicious attacks, phishing, scams, and even disgruntled employees.

Education is key to minimize vulnerabilities caused by humans. Everyone in the organization needs cybersecurity training to know their role in protecting data and digital assets. Training on awareness and procedures helps employees be more careful, more vigilant and know the right procedures to take should an incident occur.

2 Access Management

The risks associated with network and application access have increased tremendously with growth of databases, remote connectivity and wireless technologies. The fundamental principle in access control is to ensure the protection sophistication level aligns with the risk level. The greater the risk level, the stronger the access management controls should be.

3 Data Encryption

Regulations and best practices are rapidly broadening the scope of data that should be encrypted. Many organizations are challenged to understand what needs, and doesn't need, to be encrypted. Ask what data is being encrypted, and question if it is the right data.

Mobile access to systems is causing more data to reside on those devices and outside the protection of central servers. Ensure that all data touchpoints are secure, and that the right data is protected with adequate encryption.

4 Network Security

Executives and board members should know the truth about how susceptible your network is to security threats. Both public and private networks are pathways to valuable data, and are targets for security breaches.

Vulnerability scans are a first step to securing your network, but aren't enough to protect your data. Scans are risky, often result in false positives, and create alerts that are not actionable. You should insist on routine, third-party penetration tests on internal and external networks.

Hire specialists to test your network the same way hackers do – aggressively, creatively and persistently. Then work with IT to prioritize your action plan and make the right changes.

5 Operating System/ Application Security

New application and operating system vulnerabilities are discovered every day. Vendors distribute patches to repair code as they become aware of them. Keeping critical software patches installed and up to date is necessary to defend your organization from attack.

But custom, in-house applications require experienced security researchers to find vulnerabilities in the software and remediate. Most IT organizations don't have the time or resources to actively test and patch custom applications. In those situations, knowledge of weaknesses will allow you to structure your network and layer protection around your weak points to better protect your data.

6 Security Policies & Procedures

Do you understand the organization's information security strategy and recovery plan? Information security isn't just an IT issue. All executives and board members should understand the organization's information security strategy and recovery plan. In a breach, the entire organization is in danger of lost revenue, customers and damage to your reputation and brand.

Weak or non-existent security policies and procedures provide little accountability. Don't settle for basic templates to establish security policies and guidelines. Your organization needs to define actionable plans and procedures that address your unique situation and needs.

7 Third Party Relationships

Over 60% of data breaches are linked to third-party vendors. When outside partners and vendors connect into your systems through supply chain and other B2B relationships, they increase your security risks. Your vendors' security weaknesses are now your security weaknesses.

Third parties that interact with your systems must have security practices for your critical data that meet or exceed your own. Monitoring these vendors can be challenging and time consuming, so find the right expertise to help you manage this large security risk.

8 Disaster Recovery

In the face of a data breach, outage or natural disaster, you must have a proactive approach and plan to minimize data loss and recovery time. Often, the disaster recovery site is not as secure as your production site, and is a prime target for breaches.

Backing up your data without considering how that backup is transmitted, stored and recovered can expose data to additional vulnerabilities. In addition to recovery and restore plans, backup sites require incident response plans to determine why the breach or outage occurred.

HORNE Cyber Solutions understands cybersecurity. We help organizations minimize the risks associated with the threats of external cyber criminals, internal human error and even natural disasters. To learn more about how your organization can become more secure against cyber threats, visit **www.hornecyber.com**.

HORNE CYBER