Questions to Ask Regarding Security Risks

With the increasing breadth and depths of cyberattacks, companies today have many reasons for addressing information security and taking a proactive and repetitive approach. Protecting sensitive and confidential data creates an expectation for organizations to devote the utmost attention and priority to information security risks. After all, financial transactions are not the only thing that are being compromised; personal data, health information and intellectual property are now in the crosshairs.

The following questions can help assess your security program.

Data

"Only 11.1% of companies passed all 12 PCI requirements in 2013."
– 2014 Verizon PCI Compliance Report

1. Are you aware of your contractual and regulatory responsibilities if you handle health care data (HIPPA), credit card data (PCI DSS) or other confidential information and the penalties for not being fully compliant?

2. Does your organization utilize strong encryption to lock down sensitive information (personal, health care, credit card and trade secrets) in databases and servers to prevent hackers from easily stealing such data?

3. Are access controls in your organization reviewed and up to date to prevent former employees, contractors or low level users from accessing sensitive information (personal, health care, credit card and trade secrets), and is this audited?

Web Applications

"73% of intrusions were due to SQL injection and Remote Access."
– 2013 Global Security Report by Trustwave

1. Have you completed penetration testing or a vulnerability assessment in the last year to verify your internet facing systems are free from known exploits that hackers commonly take advantage of?

2. Have your software developers been trained in secure software development methodologies that prevent vulnerabilities from being introduced into custom written software applications?

3. Does your organization have a plan in place to protect against Distributed Denial of Service (DDOS) attacks, which prevent the use of critical internet applications such as e-mail, VPN or websites?

Wireless

"Using WEP is #6 on the Top 10 Network Vulnerabilities."
– 2013 Global Security Report by Trustwave

1. Does your organization utilize a BYOD (bring your own device) wireless network for user's mobile devices and understand the risks associated with such networks?

2. What wireless network security controls do you have in place to secure your network from hackers sitting in your parking lot and capturing your data?

If you would like more information on our services, please contact:

Anthony Munns
FBCS, CITP, CIRM, CISA
314.983.1297
amunns@bswllc.com

Michael Springer
CISSP, GPEN, CEH, QSA
314.983.1374
mspringer@bswllc.com

BROWN SMITH WALLACE LLC
A MEASURABLE DIFFERENCE℠

St. Louis, MO
St. Charles, MO
Glen Carbon, IL

Toll-Free 1.888.279.2792

bswllc.com

Questions to Ask Regarding
Security Risk

Systems

"2/3 of data breaches were utilizing third party System Administrators."
– 2013 Global Security Report by Trustwave

1. What assurances do you have in place that computers are regularly patched and updated to prevent your organization from being infected by a virus or malware?

2. What industry recognized security baselines and standards has your IT team used to harden your servers, desktops and networking devices?

3. Does your cloud provider have controls in place to backup your data, safeguard the privacy of your data, ensure the security of your data, and provide redundant systems so your data is always available? Have you requested their PCI DSS AOC or SOC1 or SOC2 reports?

Security Awareness

"The median number of days that the attackers were present on a victim network before detection is 234!"
– 2013 Threat Report by Mandiant

1. Do your users know how to detect a phishing or social engineering attack trying to trick them into giving away company secrets?

2. Are your users educated on how to select strong passwords and passphrases, and do they understand the risks of sharing login information with other users?

Incident Response

"In 2013, the average cost paid for each stolen account was $145."
– 2014 Cost of Data Breach Study: Global Analysis by Ponemon Institute

1. If your organization was hacked tomorrow, do you have an incident response plan in place to minimize the cost and exposure of the data breach?

2. Does your team annually review, update and test that the incident response plan is accurate to the current systems?

3. Are HR, IT, legal, marketing and management all on board and coordinated with the plan?

BROWN SMITH WALLACE LLC
A MEASURABLE DIFFERENCE™

St. Louis, MO | St. Charles, MO | Glen Carbon, IL

Toll-Free 1.888.279.2792 | info@bswllc.com | bswllc.com