PBMares℠

Cybersecurity: Minimizing A Big Threat for Small Businesses

PBMares℠

Your Future. Our Focus.

Presented by:

Harvey Johnson, CPA

Partner

Certified Public Accountants & Consultants

Today's Topics

1. Current trends in Cybersecurity
   a) Which industries are being targeted and why
   b) What hackers are looking for
2. Why Cybersecurity is a major problem for small businesses
3. Building an Effective Security Awareness Program
4. Top 10 Cybersecurity Controls for Small Businesses and Non-profits

What Is Cybersecurity?

Definitions - Cybersecurity

- **Cyberspace**
  - A global interdependent network of information system infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.
- **Cyber Attack**
  - An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of data or stealing controlled information.
- **Cybersecurity**
  - The ability to protect or defend the use of cyberspace from cyber attacks.

Why Is Cybersecurity Important?

The Facts

2015 – The Rise of PII

- Per BankInfoSecurity - In 2015 hackers began to shift their focus from targeting credit card data to obtaining Personally Identifiable Information, PII.
- This means retail attacks dropped and attacks on businesses and organizations with PII increased.

Cyber Stats

PBMares

Industries breached in 2015 and 2014

	2015	2014
Government	43%	5%
HealthCare	19%	3%
Other (*Nonprofit)	17%	3%
Technology	12%	9%
Retail	6%	55%
Education	3%	5%
Finance	1%	20%

2015 Trends

- **Discovery of zero-day vulnerabilities increased significantly.**
- In 2015, the number of zero-day vulnerabilities discovered more than doubled to 54 (one per week)
- 125% increase from the year before.

2015 Trends

- **Employee targeting doubled in spear-phishing campaigns.** Spear-phishing campaigns targeting employees increased 55% in 2015.

- **Ransomware attacks continue to rise.** Hackers have now discovered how easy it is to take hold of servers and corporate systems. Ransomware increased 35% in 2015. Ransoms are expected to increase in 2016.

There is No Such Thing as a Secure Network

- There are 2 types of breaches:
  1. Infrastructure
  2. Information
- The reality is that every company/organization will experience an infrastructure breach.
- The number of attacks and sophistication are growing at a speed that it is not a matter of if, but when.

Be Prepared

- Remember what the Buddha said – "Pain is inevitable, suffering is optional."

- An infrastructure breach is inevitable - an information breach <u>can be prevented</u> with the right control environment (monitoring, detection, training, application controls).

Be Prepared

- Information breaches are the worst kind, they can cause irreparable damage to an organization.
- 60% of organizations (small businesses) shut down within 6 months of a breach.
- Mainly because of inadequate Incident Response Plan (IRP)

Data Breach Costs (2015)

- Direct Costs of a Data Breach
  - Forensics and Recovery: $12,000 to $100,000+
  - Breach Notification (per individual): $0.50 to $5
  - Credit Monitoring (per individual): $10 to $30
  - Crisis Communications: $10,000+
  - Legal Fees: $5,000+
  - Security Updates: $15,000

Data Breach Costs – The Unquantifiable

- Additional costs of a data breach
  - Loss of business operations
  - Loss of reputation
  - Fines and penalties (government or private compliance agency)
  - Future oversight and scrutiny
  - Potential ransom payment or extortion

I'm Not Worried…
I've Got Insurance!

Does your client have cyber insurance? Even if they do, is it the right coverage? Is it enough? Types of Coverage Include:

- Website Phishing
- Extortion
- Breach Notification
- Business Interruption
- Breach Liability
- Breach Expense
- Data Restoration

It's also important to note that as more and more claims are filed, insurance companies are looking for ways to avoid paying claims. If the organization has weak IT controls…claims could be denied or limited.

Building an Effective Security Program

Building an Effective Security Awareness Program

1) Train employees on how to recognize an attack, and what to do when an attack happens.

- Policies should be designed to assume you will be compromised.
- Have a remediation plan (incident response plan/IRP).
- Train and communicate step by step instructions on what to do if an attack happens.
- Test employee awareness regularly (at least annually).

Building an Effective Security Awareness Program

2) Regularly talk to employees about cybersecurity.

- It’s not enough to require an annual review and signing of “I have read and understand the company’s IT policies.”
- Consider having quarterly updates/refreshers on different topics – CISO or Security Officer should lead this effort.

Building an Effective Security Awareness Program

3) A system is only as secure as its weakest link

- No matter the efforts to secure the network, people/employees play a vital role in its success.
- More than 75% of all attacks are traced to human error.
- Encourage cooperation, not just compliance (buy-in).
- Establish policies sophisticated enough to cover all attack vectors (risk assessments are important here).

Building an Effective Security Awareness Program

4) Warn employees about social engineering

- Do NOT click that link!
- Be aware of social media, blogs and suspicious links

Top 10 Cybersecurity Controls for Small Businesses and Nonprofits

Top 10 Cybersecurity Controls

1. Perform an information/cyber security risk assessment
   - Identifies processes and key functions that need to be secured so you can build a control environment to meet your needs
   - Identify and inventory all systems (hardware and software) that need to be monitored

Top 10 Cybersecurity Controls

2. Conduct routine Vulnerability scans (both internal and external).
   - Scans identify configuration gaps that hackers can exploit.
   - Most cyber incidents are the result of poor configuration of devices and systems.
   - Scans should be conducted at least annually.

Top 10 Cybersecurity Controls

3. Establish baseline security configurations for all hardware, software including mobile devices, laptops, workstations, servers, etc.
   - Having a baseline for security settings allows the organization to maintain consistency and reduces the risk of unauthorized content being installed on the network or devices.

Top 10 Cybersecurity Controls

4. Centralize and control configuration management and patch management.
   - Centralizing patch management allows the organization to ensure all workstations, laptops and mobile devices are up to date with the most recent anti-virus.

Top 10 Cybersecurity Controls

5. Ensure disaster recover procedures are adequate to support recovery and restoration of data in the event of a cyber attack.
   - Each system should be automatically backed up on at least a weekly basis, and more often for systems storing sensitive information.
   - The operating system, application software, and data on a machine should each be included in the overall backup procedure.
   - Test data on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.

Top 10 Cybersecurity Controls

6. Control access to systems and data based on "Need to Know" principle
   - Segment the network based on the classification level of the information on the servers.
   - Restrict access to sensitive systems or areas on the network based on job roles/responsibilities
   - Use security groups to control access within programs
   - Control and restrict third party/vendor access to systems

Top 10 Cybersecurity Controls

7. Use third party resources to supplement IT skill gaps
   - Consider out-sourcing or supplementing IT staff with vendors who specialize in network maintenance
   - Consider hiring consultants to perform risk assessments to identify control gaps/weaknesses

Top 10 Cybersecurity Controls

8. Understand third party contracts and service level agreements
   - Identify and rank third party vendors based on criticality (i.e. cloud, core, etc.)
   - Carefully review and understand third party agreements, specifically roles and responsibilities
   - Obtain and review applicable SOC reports
   - Review and implement applicable user entity controls

Top 10 Cybersecurity Controls

9. Utilize intrusion prevention/detection systems to supplement firewalls (IPS/IDS, ASA)
   - IPS/IDS/ASA systems monitor network activity and notify IT administrators of suspicious or unusual activity. They also block and quarantine suspicious items to help prevent attacks on the network.

Top 10 Cybersecurity Controls

10. Establish an Incident Response Plan (IRP)
    - Policies and procedures for handling events, including the types and severity of events
    - IRPs include: team roles and responsibilities, media and communication channels (internal/external), cyber insurance, law enforcement contacts, consultants (forensics)
    - Test the IRP through table top exercises

Contact

Harvey L. Johnson, CPA
Partner

PBMares, LLP
150 Boush Street, Suite 400
Norfolk, VA 23510
Phone: (757) 627-4644, ext. 6016
hjohnson@pbmares.com