Cybersecurity for Not-For-Profits:

WHAT YOUR BOARD MEMBERS SHOULD KNOW

OCTOBER 6, 2017

CBIZ MHM

Accounting | Tax | Advisory

Agenda

- Introduction
- Definitions & Terms
- Trends
- Case Studies
- Basic Cyber Hygiene
- Questions Leadership Should Know, Ask & Do
- Your Next Steps

Personal Background

Ray Gandy

- 30+ years in information technology
  - Global IT Audit Director
  - CIO
  - Director, Infrastructure & Security
- BSBA, Clarion University of Pennsylvania
- MBA, Rensselaer Polytechnic Institute
- GIAC Critical Controls Certification (GCCC)
- AICPA, ISACA, ISSA, SANS Institute
- AEFCU Board of Directors since 1995

☎ Direct: 617.761.0722

✉ Email: RGandy@cbiz.com

GENERAL DYNAMICS

Raytheon

United Technologies

CBIZ MHM

Definitions & Terms

- ***Critical Data*** – Important data of an entity that if stolen, lost or destroyed, may result in financial loss, operational impact, brand/reputation degradation and/or personal liability.
- ***Malware*** - Software that compromises the operation of a system by performing an unauthorized function or process.
- ***Phishing*** - Digital form of social engineering to deceive individuals into providing sensitive information.
- ***Spear Phishing*** - An e-mail spoofing fraud attempt that targets a specific organization or individual, seeking unauthorized access to confidential data. Spear phishing attempts are not typically initiated by “random hackers” but are more likely to be conducted by perpetrators out for financial gain, trade secrets or military information. These attacks are more targeted than common phishing or spam attacks.
- ***Watering Hole Attack*** - A security exploit in which the attacker seeks to compromise a specific group of end users by infecting websites that members of the group are known to visit. The goal is to infect a targeted user's computer and gain access to the network at the target's place of employment.
- ***Patching*** - A patch, sometimes just called a fix, is a small piece of software that's used to correct a problem, usually called a bug or vulnerability, within an operating system or software program.
- ***Ransomware*** - Type of malware which restricts access to the computer system that it infects, and demands a ransom paid to the creator(s) of the malware in order for the restriction to be removed.

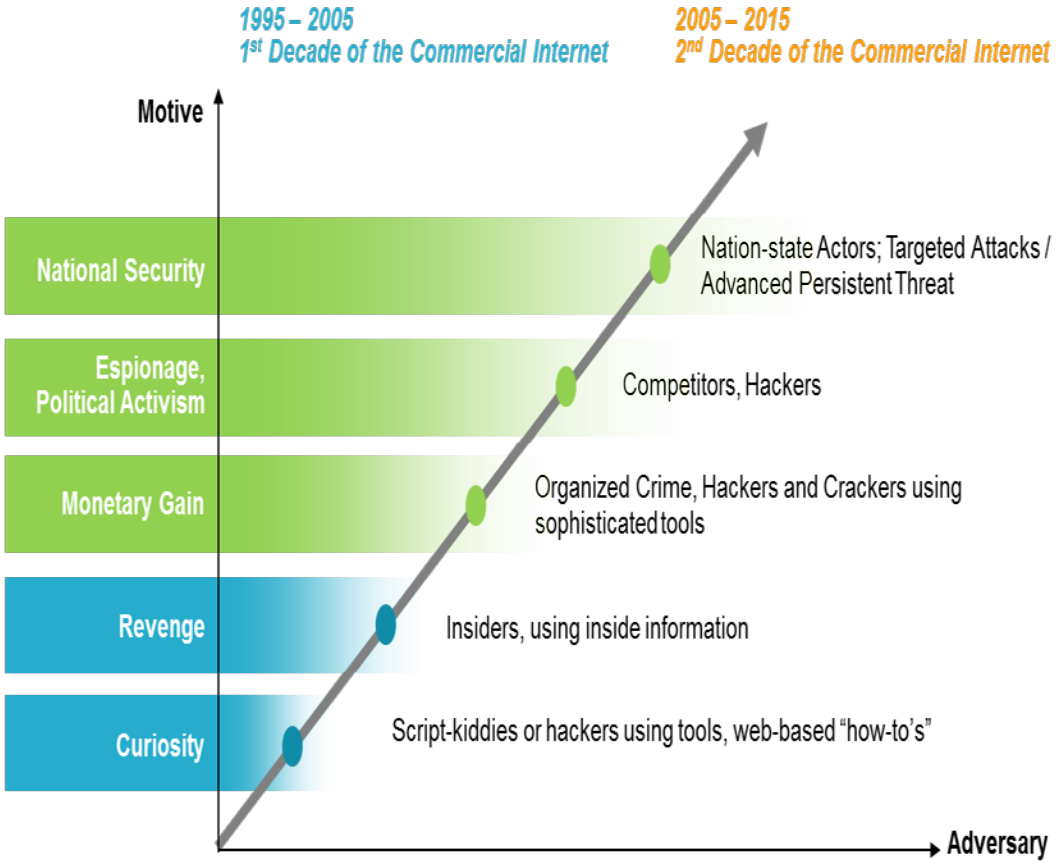
Trends

Cyber Security Threats / Actors Are Increasing

Cyber security attacks are becoming ***more sophisticated, persistent and difficult to detect.***

Security threats continue to ***evolve rapidly*** with the expansion of internet based services and mobile technology.

Early into the 3rd decade, an **increase in the number of cyber criminal attacks on SMBs** are causing significant impact and increases in cost to protect.



Source: *Verizon Data Breach Report*

Trends – Overall First Half of 2017

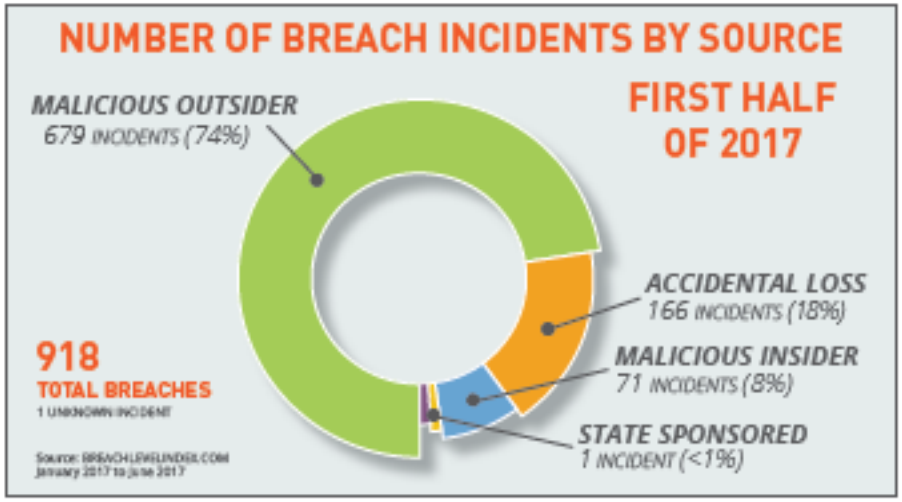
- 918 data breaches worldwide, compared with 815 in the last six months of 2016 (13% increase).
- Identity theft accounted for three quarters of data breaches (49% increase) compared to the previous six months.
- 1.9 billion data records were lost or stolen during the first half, compared with 721 million during the previous six months (164% increase).
- There were 22 breaches in which more than 1 million records were compromised, stolen, or lost in the first half of 2017.
- More than 500 data breaches (or 59% of the total) had an unknown or unreported number of compromised records.

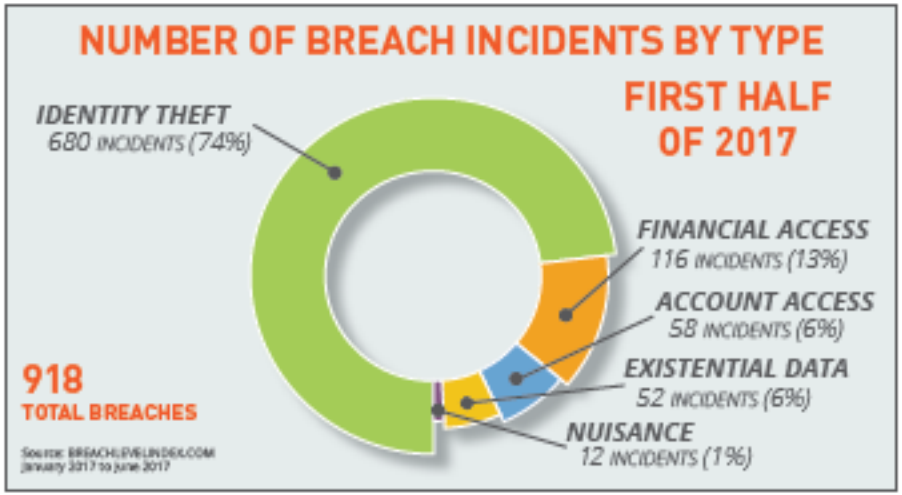
Source: *www.breachlevelindex.com*

Trends – Source & Type

- The number of breaches involving ***accidental loss*** totaled just 166, accounting for 18% of all breaches. But these attacks resulted in the theft of more than **1.6 billion records**, which accounts for a whopping 86% of all records stolen in the first half via data breaches.

- As has been the case over the past several years, **identity theft** was the most common mode of attack used in data breaches in the first half of 2017. This tactic was employed for 680 data breaches, accounting for about three quarters **(74%) of all the incidents** during the period.

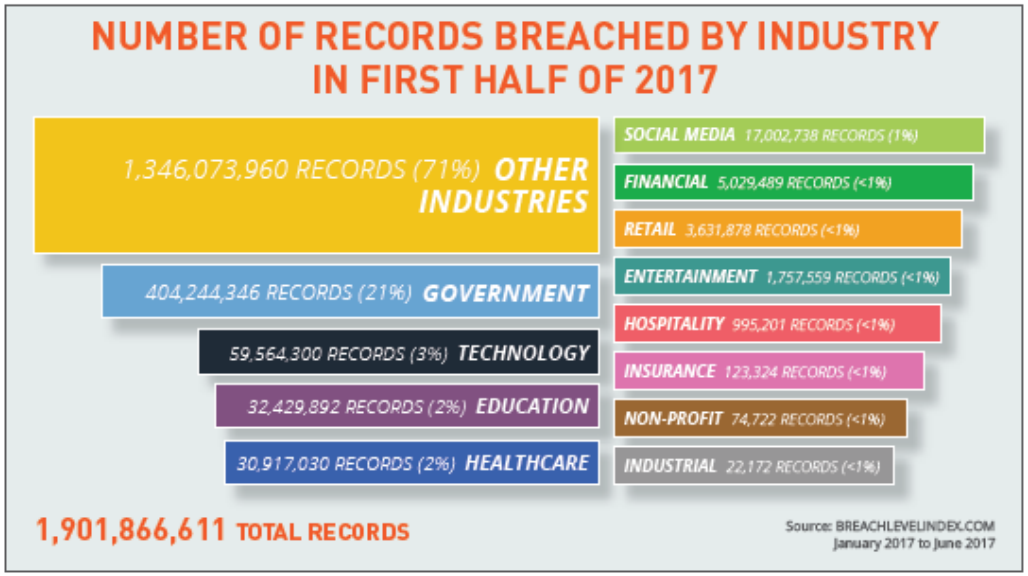




Source: *www.breachlevelindex.com*

Trends - Education

- The education sector had experienced 118 breaches (***13% of all breaches***) that impacted a total of **32 million** records (2%).
- The jump in breaches from the previous six months was significant at ***103%***.
- But the rise in the number of records involved was monumental at ***4,957%***, increasing from 641,000 records.



Source: *www.breachlevelindex.com*

Case Studies

Case Studies

Category: Educational

ITRC Breach ID	Company or Agency	State	Breach Category	Records Exposed?	Exposed # of Records
ITRC20170713-11	Auburn University	AL	Educational	Yes - Unknown #	Unknown
ITRC20170627-06	Texas Association of School Boards	TX	Educational	Yes - Published #	6,100
ITRC20170623-06	Miami-Dade County Public Schools	FL	Educational	Yes - Published #	522
ITRC20170619-05	Occidental College	CA	Educational	Yes - Unknown #	Unknown
ITRC20170614-02	Oklahoma University	OK	Educational	Yes - Unknown #	Unknown
ITRC20170612-01	Washington State University - Social & Economic Scie	WA	Educational	Yes - Published #	1,000,000
ITRC20170607-01	Northern Humboldt Union High School District	CA	Educational	Yes - Unknown #	Unknown
ITRC20170531-01	University of Alaska	AK	Educational	Yes - Published #	25,000
ITRC20170530-05	Mallard Creek High School / Charlotte-Mecklenburg Sc	NC	Educational	Yes - Unknown #	Unknown
ITRC20170525-09	Niskayuna Central School District	NY	Educational	Yes - Published #	945

Source: *www.idtheftcenter.org*

Case Studies (cont'd)

- On April 21, 2017, Washington State University learned that a locked safe containing a ***hard drive had been stolen***. ***Not*** all of the information on the drive was ***encrypted*** and it was determined that the hard drive contained personal information, including name, address, SSN, and in some cases, personal health information.

- Approximately 25,000 students, staff, and faculty members associated with the University of Alaska were affected following a successful ***phishing scam*** and subsequent data breach late last year.

- Iowa City-based University of Iowa Health Care notified patients June 22 after it discovered protected health information for roughly 5,300 had been ***available online for almost two years***, the hospital confirmed to Becker's. The hospital said a limited dataset was ***unintentionally saved in unencrypted files*** and posted online through an application development site May 2015.

- Oklahoma U unintentionally exposed thousands of students' educational records — including social security numbers, financial aid information and grades in records dating to at least 2002 — through ***lax privacy settings in a campus file-sharing network***, **violating federal law**. In just 30 of the hundreds of documents made publicly discoverable on Microsoft Office Delve, there were more than 29,000 instances in which students' private information was made public to users within OU's email system. ***Each instance could constitute a violation of the Family Educational Rights and Privacy Act,*** which gives students control over who can access their educational records.

Source: *www.idtheftcenter.org*

Case Studies (cont'd)

- Officials at MacEwan University in Edmonton, Alberta recently ***received fake emails*** that said they were from one of the school's major vendors, and that the vendor was **changing its banking information**.

- ***Three staffers*** made payments in three separate installments, according to the Toronto Star. The funds totaled **$9.5 million** or $11.8 million Canadian dollars.

- The mistake was only discovered when the ***actual client called the university***, saying it had not yet been paid.

Canadian university scammed out of $11.8 million

MacEwan University in Edmonton, Alberta, is the latest confirmed victim of scammers.

Source: *www.time.com/4924461/macewan-canadian-university-loses-10-million-email-phishing-scam*

Basic Cyber Hygiene

Basic Cyber Hygiene

- The ***Cyber Hygiene Campaign*** was developed by the Center for Internet Security (CIS), Council on CyberSecurity (CCS), working with the Department of Homeland Security (DHS), and the National Governors Association Governors Homeland Security Advisors Council (GHSAC).

- The Campaign focuses on the top 5 areas (out of 20) to address the most critical areas which, when fully implemented, can prevent 80% of all known attacks.

5 Critical Security Controls

- Network device management
- Software and applications management
- Configuration management
- Vulnerability assessment and remediation approach
- Privileged ID management

Basic Cyber Hygiene

CSC 1: Inventory of Authorized and Unauthorized Devices

Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

- Attackers wait for new and unprotected systems to be attached to the network.
- Attackers also look for devices (especially laptops) which come and go off of the enterprise's network, and get out of synch with patches or security updates.
- Attacks can take advantage of new hardware that is installed on the network one evening but not configured and patched with appropriate security updates until the following day.

Basic Cyber Hygiene

CSC 2: Inventory of Authorized and Unauthorized Software

Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

- Attackers continuously scan target organizations looking for vulnerable versions of software that can be remotely exploited.
- Some attackers also distribute hostile web pages, document files, media files, and other content via their own web pages or otherwise trustworthy third-party sites.
- Once a single machine has been exploited, attackers often use it as a staging point for collecting sensitive information from the compromised system and from other systems connected to it.

Basic Cyber Hygiene

CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

- As delivered by manufacturers and resellers, the default configurations for operating systems and applications are normally geared to ease-of-deployment and ease-of-use – not security.
- Even if a strong initial configuration is developed and installed, it must be continually managed to avoid security "decay" as software is updated or patched, new security vulnerabilities are reported, and configurations are "tweaked" to allow the installation of new software or support new operational requirements.

Basic Cyber Hygiene

CSC 4: Continuous Vulnerability Assessment and Remediation

Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

- Cyber defenders must operate in a constant stream of new information: software updates, patches, security advisories, threat bulletins, etc. Understanding and managing vulnerabilities has become a continuous activity, requiring significant time, attention, and resources.
- Attackers have access to the same information and can take advantage of gaps between the appearance of new knowledge and remediation.
- Organizations that do not scan for vulnerabilities and proactively address discovered flaws face a significant likelihood of having their computer systems compromised.

Basic Cyber Hygiene

CSC 5: Controlled Use of Administrative Privileges

The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

- The misuse of administrative privileges is a primary method for attackers to spread inside a target enterprise.
- Attackers target privileged user accounts through watering holes, phishing, and other methods. The attacker looks to install keystroke loggers, sniffers, and remote control software to find sensitive data and move throughout the network.
- If administrative privileges are loosely and widely distributed, or identical to passwords used on less critical systems, the attacker has a much easier time gaining full control of systems, because there are many more accounts that can act as avenues for the attacker to compromise administrative privileges.

Questions Leadership Should Know, Ask & Do

What to Know, Ask & Do

- Do you have an IT security strategy and plan that is aligned with your highest value information?
- What makes you feel confident in your security and controls over the company's data?
- Would your organization be able to detect a breach? How often does management review incidents and breaches and when was the last one?
- When was the last time the organization had an IT security assessment performed against a standard framework?
- When was the last time key suppliers and partners were reviewed with respect to access to data and systems?
- What investments are you making in improving your employees' understanding and everyday use regarding information security?

What to Know, Ask & Do

Do you have an IT security strategy and plan that is aligned with your highest value information?

- Documented with a roadmap, milestones and metrics.
- Designed to protect the critical data of the company that if lost, stolen or damaged beyond repair, would negatively impact the business.
- Covers all security layers of defense.
- Is aligned with a “Security Council” consisting of leadership from all areas of the business.

What to Know, Ask & Do

What makes you feel confident in your security and controls over the company's data?

- Understand the basic controls.
- Develop and review key metrics.
- Obtain independent assessments of your approach and plan.
- Understand the guidance provided by security professionals and regulatory agencies.

What to Know, Ask & Do

Would your organization be able to detect a breach? How often does management review incidents and breaches and when was the last one?

- Are you actively looking for data exfiltration?
- Do you use a Security Information and Event Management (SIEM) system?
- Do you look to share incident and breach information with other educational institutions?
- Is root cause established and adequately addressed?

What to Know, Ask & Do

When was the last time the organization had an IT security assessment performed against a standard framework?

- NIST, CIS 20, PCI, HIPAA, ISO 27001/02, FFIEC, etc.
- Leverage an independent reviewer.
- Establish a baseline and continue the journey from there.
- Don’t be alarmed by “poor” results.

What to Know, Ask & Do

When was the last time key suppliers and partners were reviewed with respect to access to data and systems?

- Periodically review which outside parties have access to which systems, and the controls in place to protect that access.
- Review your contracts regarding third party control and security of your data.
- Establish minimum cybersecurity practices for each vendor to meet and regularly evaluate that they meet the requirements.
- Ensure your company is a part of the vendor's notification chain should the vendor experience a breach or cybersecurity incident.

What to Know, Ask & Do

What investments are you making in improving your employees' understanding and everyday use regarding information security?

- Ensure that you communicate to staff on a regular basis (not just at onboarding) the information they need to know about their role in cybersecurity.
- Consider notifying employees about emerging threats, particularly ones that involve social engineering such as phishing emails.
- Consider conducting simulated social engineering exercises to see how employees respond to a typical attack, such as a phishing email. Schedules should also be put in place for ongoing cybersecurity awareness training.

Your Next Steps

Sophistication and frequency of attacks are increasing. The effects are damaging and can be devastating. Everyone - boards of directors, company leadership, IT – plays a critical role in cybersecurity risk management.

Having an enterprise-wide approach to mitigate information security threats is a proven best practice in protecting valuable data assets. A comprehensive security assessment should be performed to substantively review all controls in the environment and to establish an ongoing benchmark for improvement.

Begin the journey…start the conversation

Be involved…stay involved

Look to share information with others

Be patient and vigilant…it takes time

QUESTIONS