ANCHIN

Your Expert Partner

CPE for CFOs: Cybersecurity

Anthony M. Bracco, CPA/CFF, CFE, CVA, CGMA
Daniel Stieglitz, CPA-CITP

November 3, 2016

Cybersecurity

- Types of Breaches
  - What are they?
  - What are you most susceptible to?
  - How do you protect yourself?
  - What do you do if you suffer a breach?
- Insurance Coverage
  - Will your carrier cover you when you need it?
- AICPA – Defining auditor responsibilities regarding cyber security

ANCHIN
Your Expert Partner

Cybersecurity

- Types of Security Breaches
  - Hacking
  - Phishing
  - Ransomeware
  - Human Error
  - Theft/Loss of Laptop

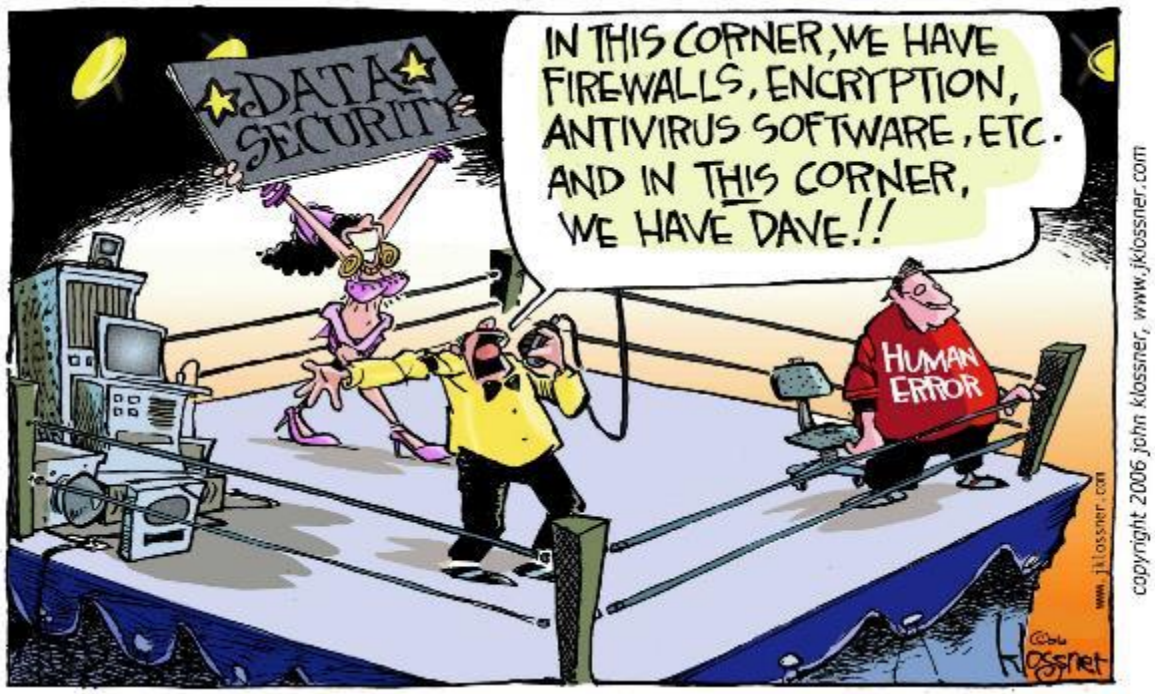
ANCHIN
Your Expert Partner

Cybersecurity

- What are we seeing?
  - Phishing
  - Hacking
    - Intercepting email
  - Ransomware

ANCHIN
Your Expert Partner

Cyber Risk – It's not just about IT



ANCHIN
Your Expert Partner

Cyber Risk

It is not just about the technology

Testing and knowing the risks related to the human factor (your employees) is a vital component when building your IT risk and compliance programs

ANCHIN
Your Expert Partner

Statistics on Cyber Terrorism

- The Securities and Exchange Commission's Office of Compliance Inspections and Examinations (OCIE) found that 74 percent of advisors and 88 percent of brokers experienced a cyber attack in 2015.
- 30 percent of all cyber attacks target financial services companies.
- According to the Verizon 2015 Data Breach Investigations Report, 525 separate incidents of cyber attack, often in the form of cyber-espionage, were reported in the manufacturing industry. This number is more than double the 251 incidents reported in 2014.

ANCHIN
Your Expert Partner

Statistics on Cyber Terrorism - continued

- Accounting Today - Cybercrime is now the second most reported economic crime worldwide and has negatively affected **at least a third** of all U.S. companies.
- According to a recent **IBM-sponsored study** by the Michigan-based Ponemon Institute, the average total cost of a data breach in 2015 was $6.5 million, with an average cost per lost or stolen record of $217. The more records lost, the higher the cost of the data breach.

ANCHIN
Your Expert Partner

Cyber Crime by industry

Top 7 industries affected by Cyber Crime:

- Banking, Capital Markets, and Investment Management
- Retail
- Communication – Internet providers – Yahoo, Google, Etc.
- Financial Services
- Hospitality and Government – tie for the 5th and 6th spot
- Manufacturing

ANCHIN
Your Expert Partner

Stats for C Level Executives

- 32% of all U.S. companies have been affected by an attack
- Only 37% of companies in the U.S. have an incident response plan
- 61% of CEOs in a national survey are concerned about what their companies are doing about cyber security
- But, only half the board members of the companies these CEOs represent actually ask about their companies' plans during their board meetings

ANCHIN
Your Expert Partner

Does Size Matter?

"Truth be told it is the data that makes a business attractive, not the size – especially if it is the Yummy data, such as lots of customer contact info (social security numbers and personal information), credit card data, health data, or valuable intellectual property."

Does Size Matter?

But most experts will also say that the reality is small and midsized enterprises (SMEs) can be more attractive targets because they tend to be less secure.

The automated processes used by cyber criminals today can mass produce attacks for little investment but great results. They are knocking on your doors.

ANCHIN
Your Expert Partner

Small Business

"Small business is a huge target because attacks are automated. The criminals don't care who they're attacking, and while any given business isn't worth much, they have viruses and ransomware that allow them to attack thousands or millions of companies quickly and can leave you paralyzed."

Those victimized by automated attacks tend to fall into what experts call the "low-hanging fruit". SMEs tend to be a much easier target for this type of attack than larger enterprises.

Most of these attacks are successful for the criminal due to a lack of employee training, which causes the employee to launch the attack and then never report the incident.

ANCHIN
Your Expert Partner

What Makes YOU attractive

- Lack of time, budget and expertise to implement comprehensive security defenses.
- Lack of policies and policy enforcement – Bring Your Own Device (BYOD) is a large concern as you connect your employees' smart phones to your email and servers
- Lack of risk awareness.
- Lack of employee training.
- Failure to keep security defenses updated.
- Outsourcing security to unqualified contractors or system administrators – Third party vendor verification
- Failure to secure endpoints.

ANCHIN
Your Expert Partner

Some things YOU can do

- Take an inventory of your information assets – what is most important to you – make sure it is locked away and protected but, within your reach. Make sure you have proper backups with version controls and archiving.
- Know your employees – give them clear direction – don't expect that they will know what to do. Document a plan for your company and make them part of it.
- Make sure you have strong locks
  - Password should be secure – and changed frequently
  - Emails with vital information should be encrypted
  - Printed copies with vital information should be properly shredded or stored secured under lock and key.
- Jiggle the locks – once a year – do a vulnerability assessment or testing of your network and your employees' response to an attack

ANCHIN
Your Expert Partner

Some more things YOU can do

- Have a plan – let's not stop at just putting up smoke detectors – in case of fire – but lets have an action plan to get us out of the building.
- Monitor who you let in – ask your third party IT vendor the same questions you would ask yourself. This includes our web developers and our hardware and application support services vendors.
- Compliance counts also – be sure that if there are laws governing your business you follow them – violations can be expensive and disruptive
- Talk to others – if you belong to any other professional development groups ask what they are doing – things change so fast in the world of Cyber – so it is vital to be proactive.

ANCHIN
Your Expert Partner

Questions ?

Anthony M. Bracco, CPA/CFF, CFE, CVA, CGMA
Anchin, Block & Anchin LLP
Anthony.Bracco@anchin.com
212-840-3456

Daniel Stieglitz, CPA-CITP
Anchin Block & Anchin LLP
Daniel.Stieglitz@anchin.com
212-840-3456

ANCHIN
Your Expert Partner