ICYMI: IN CASE YOU MISSED IT

FIRM ALUMNI SESSION:

Cybersecurity-What You Don't Know *Can* Hurt You

April 26, 2016
Hope Connections for Cancer Support, Beaumont House at FASEB

Moderator: Jason Green, Co-founder of SkillSmart, Inc.

Panelists:
Mike Raftery, Vice President of Technology Services, 501cTECH
Kimberly Gay-Armour, CPCU, Insurance Manager, Montgomery County Government, Department of Finance/Risk Management
Matthew Bergman, Attorney at Law, Co-Chair, Cybersecurity Practice Group, Shulman, Rogers, Gandal, Pordy & Ecker, P.A.
Meghan Mullee, Senior Associate Broker of Corporate & Commercial Risk, Alliant Americas

Mike Raftery: The Nonprofit Experience

You need to know the state of cybersecurity in the modern world: not “we might get hacked” but “we will get hacked.”

At one time cyberthreats were more random, now they are organized and targeted attacks. Malware is not catching it fast enough. Hackers may assume that nonprofits are not as well protected.

Five key areas to focus on (from the NIST framework for cybersecurity)

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

Your data is an asset – you have to control and protect that asset. Make sure the doors are locked (firewall), know where the windows are and know who has the keys. Bring in consultants to help you navigate the process. Eighty percent of the work is organizational–identifying what data is valuable and what is not, understanding your own risk, and assessing your systems.

Kimberly Gay-Armour: The County Perspective

All Montgomery County contracts must go through an assessment in the Department of Finance/Risk Management for insurance requirements. The county's concern is to protect the citizens of Montgomery County.

Insurance requirements for cybersecurity vary depending on the type of service being provided.

Anything that involves the use or transmission of Personal Identifiable Information (PII) or Personal Health Information (PHI) will require cybersecurity.

This includes any services related to medical health and mental health, but can also include any case where credit card information is used.

Nonprofits should check their agreements with vendors including credit card processing companies to make sure there are adequate protections in the contracts.

Matthew S. Bergman: How to Mitigate Cyber Exposure

You have a legal obligation to comply with the law. In Maryland this means you are required to implement and maintain reasonable security practices. Speak to a consultant—preferably an attorney.

Each organization should have a **WISP (Written Information Security Plan)**, which outlines an organization's plan for cybersecurity:

1. Who is responsible
2. What protocols are in place
3. How staff are trained
4. What to do in case of a suspected breach

Nonprofits are at great risk, so in spite of cost concerns be sure to bring in the appropriate expertise to help you manage this.

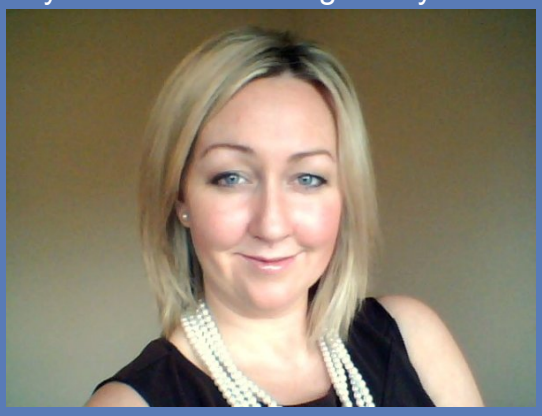
Make sure people in your organization know what to do, and how to be vigilant against social engineering attacks.

Meghan Mullee: The Insurance Perspective

Purchasing cyber insurance is like purchasing any other policy. You have to identify your risk. What would be the fallout of a breach—financial, reputational?

Coverages available in a cyberinsurance policy may include:

1. Privacy Notification & Crisis Management expenses: this generally covers a "breach coach" to help you assess and react. It may include forensic IT and an attorney to manage statutory notification requirements in various states. Coverage can include the cost of notifying individuals, PR and credit monitoring.
2. Regulatory defense & penalties: if you are investigated by any state or federal regulatory agencies this pays for defense costs and fines you might incur.
3. Data restoration & recovery: pays for IT help to restore your files, backups.
4. Business interruption & extra expense: if your business suffers (lost revenue) as the result of a breach.
5. Cyber extortion: Responds to ransom demands made after unauthorized access to your data, website, or computer system.
6. Privacy liability & information security. Coverage for defense and damages arising from third party claims as a result of unauthorized access to data, transmission of virus or malicious code, or other similar allegation.



JASON GREEN ASKS: WHAT'S ONE PIECE OF ADVICE YOU WOULD GIVE NONPROFITS?

Matthew Berg: Hire a lawyer. Exhibit and practice good computer hygiene—good training for employees so they understand the risk, put a team of experts in place ahead of time so you are prepared.

Mike Raftery: IT insecurity costs money. Nonprofits should budget and plan for cybersecurity. Reacting after you have a problem will cost much more in the long run.

Meghan Mullee: Use the free resources that come with purchasing a cyber policy. Many policies will give you a free consultation with a breach coach, will provide educational resources, and may have partner organizations with reduced rates for forensics and system testing.

Kimberly Gay-Armour: Be sure to talk to your board of directors about cybersecurity. Ultimately they are responsible for making sure the organization is protected. Bring them into the discussion so they can be part of budgeting for the solution.