proarch

Cybersecurity Roundtable:

Building Cyber Resiliency in a Threat Dominated World

Moderator

Michael Montagliano,
Chief of Innovation

MEET OUR PANELISTS

Peter Hotchkiss

Director of IT

Barclay Damon

Andrew Luna

Corporate Compliance Officer

IHI Power Services Corp.

Ben Wilcox

Chief Technology Officer
of Security & Cloud

ProArch

proarch

Question #1

proarch

What are some ways to effectively educate and communicate risk posture to the board and top execs?

What are some ways to effectively educate and communicate risk posture to the board and top execs?

Andrew

- Change the focus
- Bring IT/Cybersecurity into your compliance program
- Look at your IT and security programs as a compliance line item to receive top priority

Ben

- Set expectations: Cybersecurity is protecting data confidentiality, integrity, and availability (CIA)
- Perform a risk assessment on systems that have those types of data
- Report on findings metrics. What is the organization risk/exposure? How does risk equate to loss of CIA? How does risk reduction applies to cost to enable CIA?

proarch

Question #2

proarch

In terms of investment, what key areas of threat protection deliver the greatest return? What are the ‘biggest wins’ to prioritize in the budget that have the greatest impact on risk reduction?

In terms of investment, what key areas of threat protection deliver the greatest return? What are the ‘biggest wins’ to prioritize in the budget that have the greatest impact on risk reduction?

Peter

- Web filtering – Umbrella for protection on and off network
- Log aggregation and alerting – cut down on “alert fatigue”
- Next generation threat protection on endpoints.

Ben

- Attack Surface reduction
  - Security Awareness Training
  - Vulnerability Management
  - Advanced Email Protection to stop Phishing
- Response based tools in Managed Detection and Response
  - Endpoint Detect Platforms
  - Identity Protection

proarch

Question #3

proarch

[Energy]

Power plants reside predominantly in remote locations and have very few or no personnel on site. How can remote access be implemented in a secure way?

Power plants reside predominantly in remote locations and have very few or no personnel on site. How can remote access be implemented in a secure way?

Andrew

- Multi Factor Authentication (MFA) or Multi Point Authentication are critical
- MFA is vital to keeping attackers away- will try an easier target

Ben

- Unique accounts - no more shared
- Multi Factor
- Role based access controls
- On-site approval for vendors / 3rd parties – no unrestricted unauthorized access

proarch

Question #4

proarch

[Legal]

Law firms handle an immense amount of sensitive client data and confidential information. What data protection controls are most important so that users can still do their work, but IT has the control and security they need?

What data protection controls are most important so that users can still do their work, but IT has the control and security they need?

Peter

- Secure document management system (DMS)
  - Granular security
  - Activity logging
- Secure file sharing
- Ethical walls system to enforce and maintain walls

Ben

- Data Stewards and Ownership Assignments along with organization buy-in
- Data Governance Plan
- Technical controls to apply sensitivity, protection from loss, and retain data

proarch

Question #5

When it comes to ownership- what types of things are in the best interest of the business to say ‘let’s outsource this’ or ‘let’s take this on ourselves’?

When it comes to ownership- what types of things are in the best interest of the business to say ‘let’s outsource this’ or ‘let’s take this on ourselves’?

Peter

- Do we have the expertise?
- Can we develop it?
- Does it require direct interaction with our attorneys and staff?

Andrew

- Start with minimum outside assistance
- Have your team live it, question it, and understand it
- Then, bring external IT company in to do what they do best

proarch

Question #6

proarch

What's one piece of advice you have for other organizations who are trying to take the next step with the maturity of their security program?

What's one piece of advice you have for other organizations who are trying to take the next step with the maturity of their security program?

Peter

- Find trustworthy people that cut through the hype and marketing
- Have the people who advise you also assist in the event of an incident

Andrew

- Make your security program personal and relatable
- Help users overcome confusion and make the best decisions possible
- Learn together- not just IT's responsibility

Ben

- Assign internal ownership of Organization Security
- Supplement externally to fill the gaps in your internal team
- Security happens 24/7, be prepared
- It's not just a technology thing, make sure to include people and processes.

proarch

Open Q&A