Cyber Insurance

Panelists

- David Cole (moderator), FMG
- Kurt Suhs, CyberOps
- Bolanle Akinrimisi, Beasley
- Chris Owens, Epic
- Scott Godes, BT

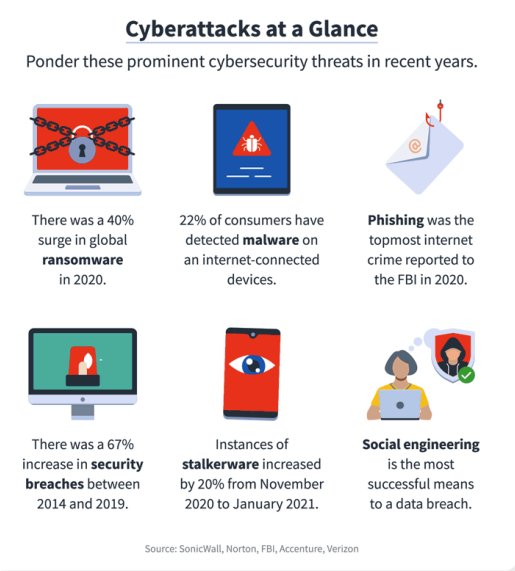
History of Cyber Insurance

- Origins of cyber insurance
- Current state of the market
- How did we get here?

Why have cyber insurance?

- 88% of organizations face spear phishing attempts in a single year — that means many businesses could be targeted by spear phishing attacks every day.
- 2,200 cyber attacks/ day = 1 cyber attack every 39 seconds

Source: us.Norton.com



The Cost of Cybercrimes

Internet crime victim losses in 2020:	**$4.2 billion**
The average cost of a ransomware attack:	**$1.85 million**
Global cybercrime damages per second:	**$190,000**
The average cost of cybercrime for organizations:	**$13 million**

Source: FBI, Sophos, Cybersecurity Ventures, Accenture

What does the claims process look like?

- Engaging breach counsel
- Engage forensics firm
- Regular communication with claims professional to ensure coverage

What types of claims do you see?

- Ransonware
- Business email compromise
- Biometrics
- Wire fraud
- Dumpster diving paper data breach

How to evaluate policy coverage and vendors BEFORE a security incident?

- Have a plan!
- Interview and pick law firm and forensics firm BEFORE you need them
- How can I contact service providers in the middle of an attack when my email is unavailable?

How is risk being evaluated?

- Risk management
- What can be done better?
- How to evaluate the risk factors for an organization
- Security controls – MFA minimum

HOT TOPIC: Should you pay the ransom?

- Restrictions to paying
- Coverage for ransom payments
- Considerations for business decision to pay or not

What does the future hold?

- Cyber market?
- Ability to get insurance
- What will be required for coverage?

Q & A