Cyber Security
You Are Okay, Until You're Not

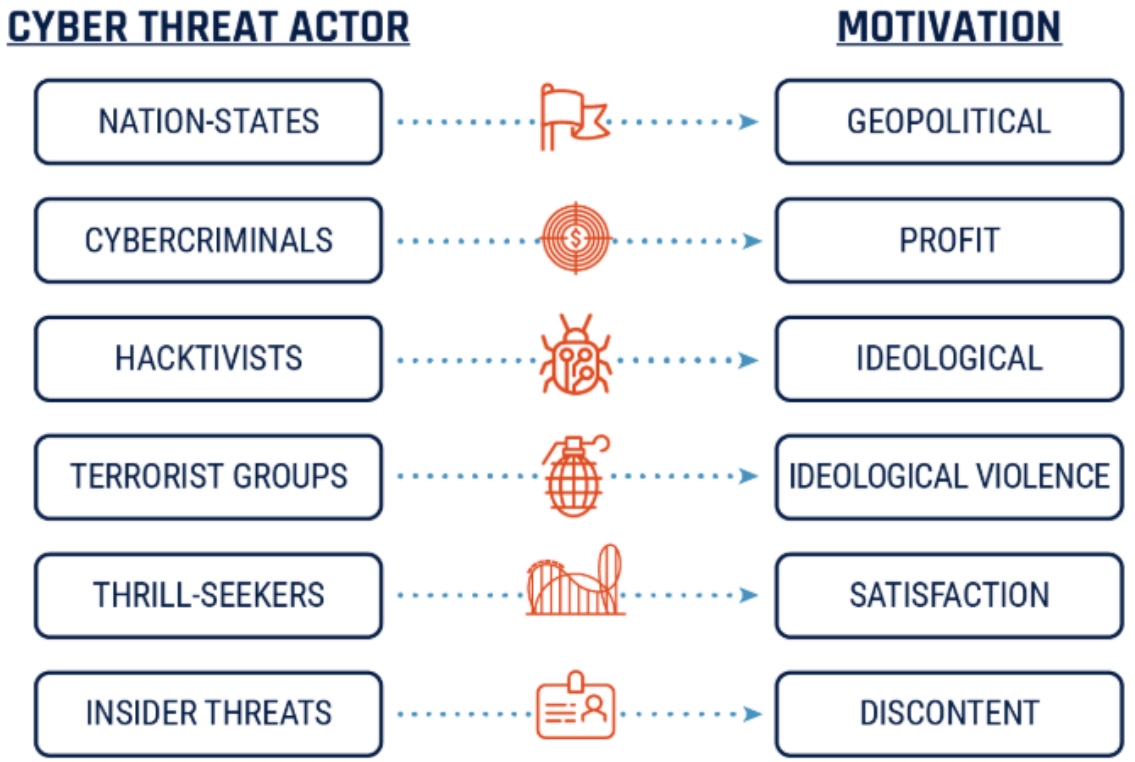
Ed Shanker
President/CEO
Meeting Tree Computer

The Stakes Are High

- About 70% of business-people have experienced data loss due to accidental deletion, disk or system failure, viruses, fire or some other disaster
- 93% of companies that lost their data for 10 days or more filed for bankruptcy within one year of the disaster and 50% filed for bankruptcy immediately
- There is a hacker attack every 39 seconds
- Malware (Trojans, adware, ransomware) continues to be the largest threat activity launched by threat actors
- Phishing attacks dominate the threat landscape – emails relayed through botnets with almost no attribution to their original sources
- The total cost of cyber crime committed globally added up to over $1 trillion in 2018

Threat Actors

Awareness of the threat actors and their motivation increases understanding of their methods, techniques and targets



RISK

The nature of a cyber security strategy depends on the level of risk the organization is prepared to take.

Sample Security Technology Stack

Protect Your Business In Layers

Policies/Procedures/
Training

Firewall/Wi-Fi
Access/separation

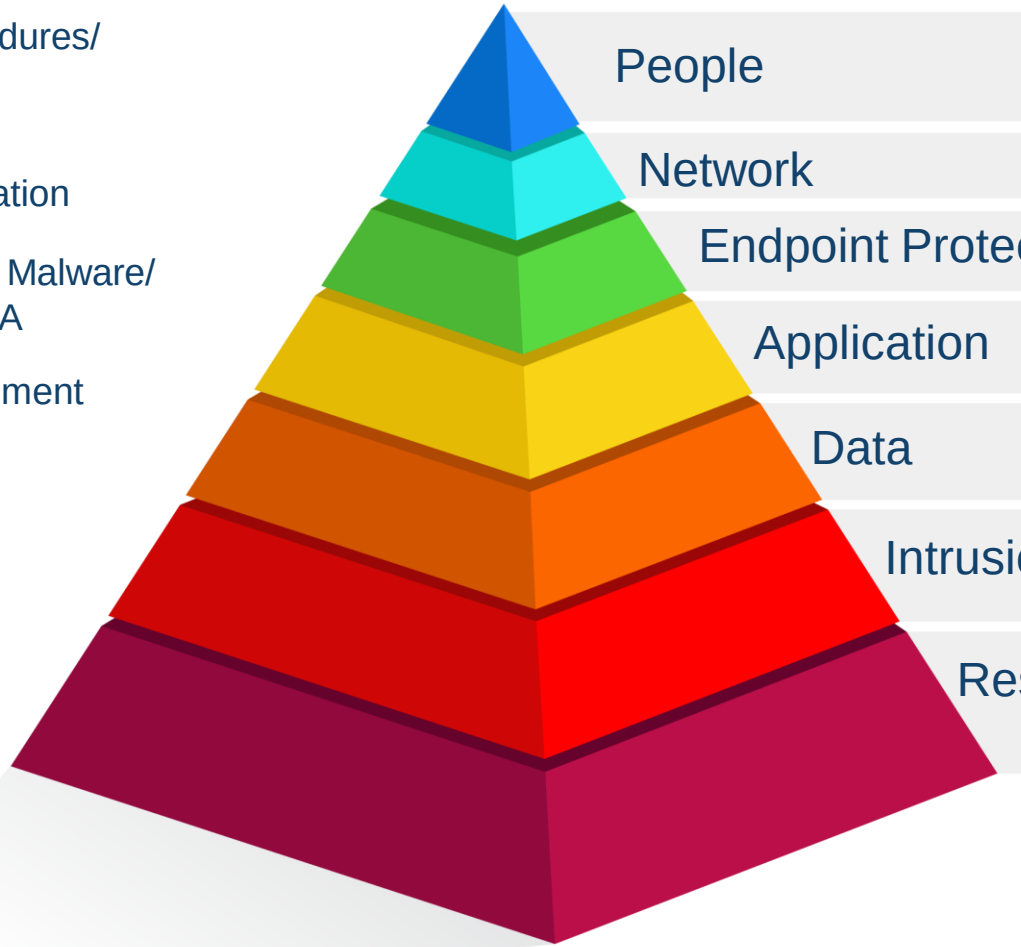
Anti Virus/Anti Malware/
Encryption/MFA

Patch Management

Encryption

SIEM/SOC

Back Up/
Business
Continuity



People 1

Network 2

Endpoint Protection 3

Application 4

Data 5

Intrusion Detection 6

Response 7

HVTECHFEST 2019

Security Stack Considerations

Cost

Complexity

Compliance

Continuity

Balance

Designing a security stack must consider the cost of implementation, weighed against the potential loss of data, time, money, and confidence caused by an incident, as well as penalties for non-compliance.

Organization

- Designate employee in charge of security.
- Establish security and acceptable use policies.
- Conduct regular security awareness training to educate employees about risks.
- Insurance.

Minimum Best Practices

- Install OS & 3rd party patches.
- Maintain Rigorous identity and access controls based on the principle of least privilege.
- Stop using RDP.
- Establish good password policy.

Machine Level

- Anti-virus.
- MFA/password management (SSO SAML Oauth).
- Advanced Persistent Threat detection.
- DNS protection, if not on firewall.
- Encryption.

Email – prime vector!

- SPAM/virus filter
- Phishing protection
- In transit encryption
- Backup
- Archive (for compliance)

Site / Edge

- Firewall – intrusion detection, intrusion prevention, data loss prevention, DNS protection, logging.
- Dark Web monitoring.
- Backup / Business Continuity.

Larger Company or Compliance Requirements

- SIEM/SOC.
- Employee monitoring.

Continuity

No defense is infallible. Any security solution must plan for failure. We must account for how we need to respond in a worst case. The plan must include policies and procedures to meet compliance obligations, contingency plans for backup and operations, and insurance.

“Changes in technology, the threat landscape and regulations create a dynamic situation that requires constant oversight and action”

OPTIV 2019 - Cyber Threat Intelligence Estimate

HVTECHFEST 2019

Conclusion

The threat is real and increasing, traditional security is not sufficient. Protecting the small business, threat avoidance and mitigation, requires cultivating an awareness and culture of security.

The security stack must be built with the assets to protect, the resources of the company to deploy, including money and personnel, and the compliance obligations, in mind.

Questions?

(845) 237-2117
Eshanker@meetingtreecomputer.com

OpenHub
Innovation | Collaboration | Education

SUNY ORANGE

Mount Saint Mary College

ORANGE COUNTY
NEW YORK
1 NOVEMBER 1683