Virtual CONSULT

Presented By

security specifiers®

SIA
SECURITY INDUSTRY ASSOCIATION

securityspecifiers
CONSULT 2020
VIRTUAL TECHNICAL SECURITY SYMPOSIUM

Plugging into Managed Services

Sponsored by

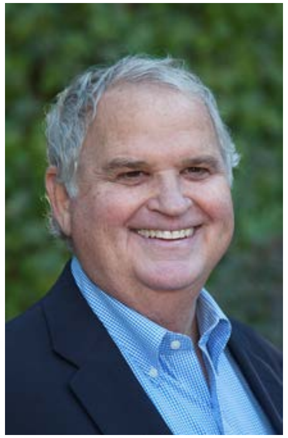
brivo®
simply better security

securityspecifiers
CONSULT 2020
VIRTUAL TECHNICAL SECURITY SYMPOSIUM

Moderator

Dan Dunkel
Managing Director,
Managed Security Services Practice
PSA Security Network

Panelists



Bud Broomhead
CEO, Viakoo

David Lathrop
Vice President
Unlimited Technologies

Gary Hoffner
Vice President
PSLA

Steve Van Till
President & CEO
Brivo

Learning Objectives: Consulting Trends

Understand the types of services that qualify as “managed”.

Describe how managed services are delivered remotely?

Explain potential security vulnerabilities and considerations in remote delivery of services.

Describe how the provision of managed services can provide enhanced system reliability.

List the pros and cons of remote managed systems vs. on-site maintenance.

Explain why the availability of remote managed services should be of interest to a design consultant during the system design phase and contracting phase of a project.

Explain the sufficiency of remote managed services during a lockdown event, such as the current pandemic.

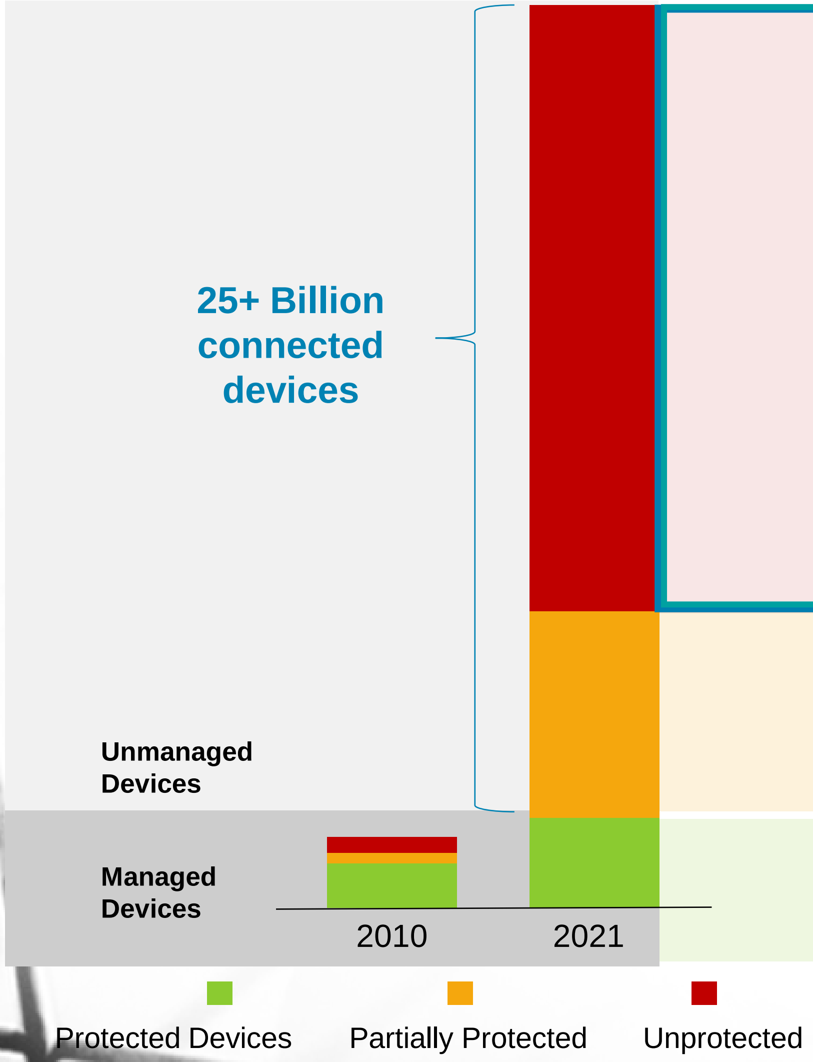
Position the industry for future opportunities

2021 SECURITY MEGATRENDS™

1. Artificial Intelligence
2. Cybersecurity of Physical Security
3. Predictive Data Analytics
4. Connectivity and the IoT of Everything
5. Cloud Computing
6. Touchless & Frictionless Solutions
7. Facial Recognition
8. Responsive Environments & Intelligent Spaces
9. Emphasis on Data Privacy
10. Move to Service Models

Unmanaged IoT Devices are a Popular Attack Vector

Discovery and Management



Unmanaged & IoT Devices

- Scanners
- VOIP
- Switches
- Printers
- Point of Sale
- Medical Devices
- Manufacturing
- Card Access
- Security Cameras
- Access Points
- Bluetooth
- Smart TVs
- Smart HVAC
- Smart Lighting

BYOD (PC and Mobile)

- Tablets
- Smartphones
- Laptops

Traditional Enterprise Devices

- PCs
- Servers
- Web

Viakoo Makes Things Work Securely

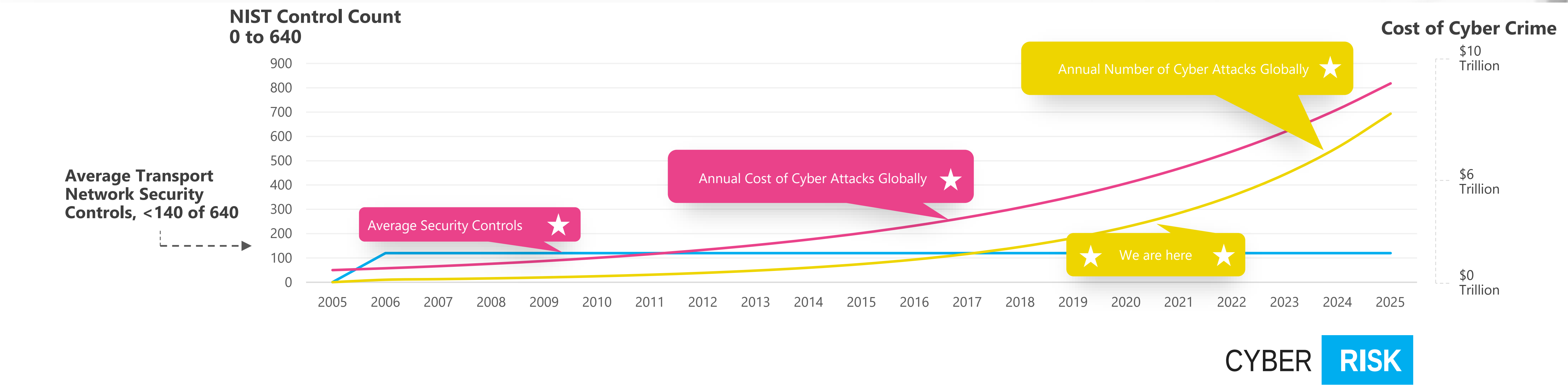
- Availability and performance (Service Assurance)
- Certificate management (SSL/TLS, 802.1x)
- Firmware patching compliance
- Password policy compliance

***Chart source*: Armis Security**

Risk Based Management Framework

The Risk Management Framework provides a process that integrates security and risk management activities into the system wide development life cycle. The risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, standards, or regulations. The following activities related to managing organizational risk are paramount to an effective information security program and can be applied to both new and legacy systems within the context of the system development and life cycle

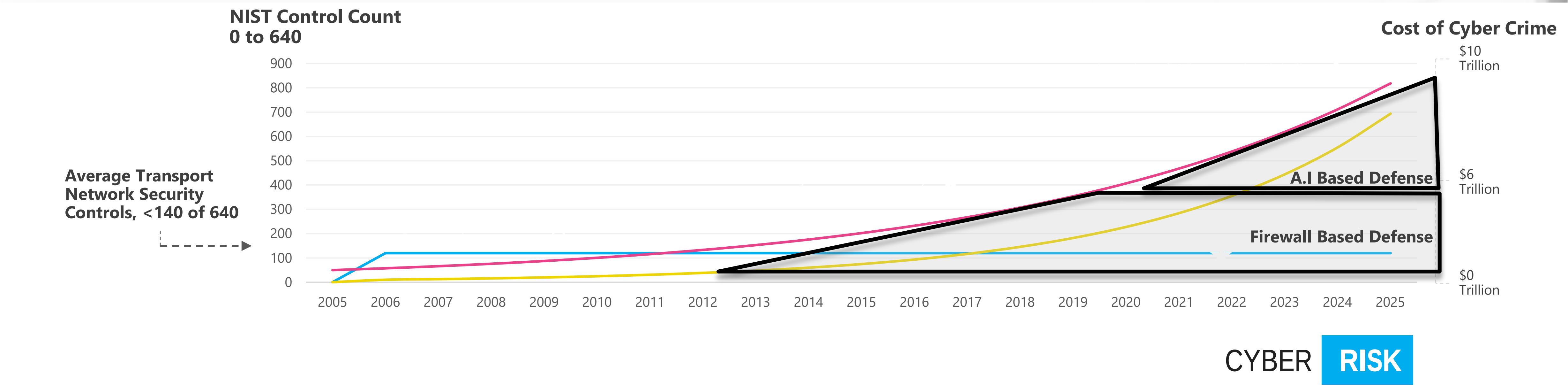
Risk , Standards & The Future of Cyber Security



Machine on Machine Learning In the Hands of the Bad Guys

One Bad Actor can now orchestrate a largescale attack campaign against any target and Nation States can now use A.I. to pass your firewalls and attack all your assets on a day to day bases.

Risk , Standards & The Future of Cyber Security (Risk Based Budgets)



A.I. and Asset Management tools are now a MUST HAVE

On Feb. 11, 2019, President Donald J. Trump issued the Executive Order on Maintaining American Leadership in Artificial Intelligence.

- on a day to day bases.
- A.I. and Asset Management tools now a MUST HAVE

Positioning Cybersecurity as a Managed Service

The Digital Risk Discussion (*Positioning cybersecurity as "digital risk"*)

#1 "Digital Communications" have fundamentally redefined the concept of business risk. As we collectively turned to digital infrastructure for the benefits of information sharing and work efficiencies, we ushered in the era of digital crime.

#2 Understanding of current and emerging digital risks to their businesses.

#3 Options for deploying effective risk countermeasures.

#4 The roll of executive leadership in creating a cybersecurity culture.

As cameras, access control, sensors and alarms are connected to the network the cybersecurity requirement is "obvious & immediate". (*RMR opportunity*)

Cybersecurity talent is not available for SMB, (who are #1 target), outsourced managed services are in demand. (*RMR opportunity*)