cyber:secured forum

JULY 29 – 31, 2019 | DALLAS, TX

Cyber:Secured Forum

2019 Highlights

Summary Findings, Session Notes and Perspectives
From Cyber:Secured Forum

Presented by

ISC INTERNATIONAL SECURITY CONFERENCE & EXPOSITION

PSA SECURITY NETWORK

SIA SECURITY INDUSTRY ASSOCIATION

cybersecuredforum.com

cyber:secured forum

JULY 29 – 31, 2019 | DALLAS, TX

Presented by

ISC International Security Conference & Exposition

PSA Security Network

SIA Security Industry Association

Quoted at Cyber:Secured Forum

Quips, snippets and wisdom from the stage of Cyber:Secured Forum

> Encryption is not an option – it's a must.
>
> – *Jimmie Lee, Facebook*

> In the financial services industry, security is the #1 thing they are spending money on today.
>
> – *David Stevens, HyTrust*

> I need to be able to feel secure when I put a physical security device on our network.
>
> – *Arve Kjoelen, McAfee*

> The 'S' in IoT is for 'security.' But there is no 'S' in IoT.
>
> – *Mark Weatheford, Booking Holdings*

> To be secure, we all need to share. We need to build security communities.
>
> – *George Finney, Southern Methodist University*

> Yes, we have a talent problem. We need to be talking to our community, talking to our schools, talking to our political leaders, because we need more momentum and the problem is only going to get bigger.
>
> – *Mark Weatherford, Booking Holdings*

> When new technologies come out, I ask, 'How can this help me and how can this hurt me?'
>
> – *William P. Woods, McAfee*

> Remember that an effective security program is an ongoing process.
>
> – *Valerie Thomas, Securicon*

> Something that was cutting edge as an attack a month ago is now available for sale.
>
> – *Eldon Sprickerhoff, eSentire*

> Cybersecurity is critically important if we're going to continue to move at the pace we're moving with digital solutions.
>
> – *Larry Wilson, University of Massachusetts*

> This is a team effort! An organization must employ a hive mentality to ensure the safety of people and data.
>
> – *Andrew Lanning, InfraGard Hawaii Member Alliance*

> Why would a well-funded cybersecurity company want to work with a physical security integrator? Most of these companies are new organizations, and the physical security industry is very mature, so it's a base of business they need.
>
> – *Bill Bozeman, PSA Security Network*

cyber secured forum

JULY 29 – 31, 2019 | DALLAS, TX

Presented by

ISC International Security Conference & Exposition

PSA Security Network

SIA Security Industry Association

We Thank You for Your Support!

Silver Sponsors

ALLEGION

BOSCH Invented for life

DELL Technologies

HID

intel

LifeSafety Power

MERCURY SECURITY part of HID Global

SECURE UTILITY

Bronze Sponsors

Altronix

AXIS COMMUNICATIONS

brivo

dahua TECHNOLOGY

Hanwha Techwin America

HIKVISION

PELCO by Schneider Electric

SMU

VIAKOO

Media Sponsors

CIO APPLICATIONS

ENTERPRISE SECURITY

SDM

SECURITY BUSINESS

SECURITY SYSTEMS NEWS

SECURITY today

Summary of Sessions

Opening Keynote – IoT, Convergence and Supply Chain Risk: Let's Not Forget "The Cyber"

Speaker:
Mark Weatherford, *Global Information Security Strategist, Booking Holdings*

Summary:
In the opening address, Weatherford challenged attendees to focus their security on the economics and the money, and not the technology. Despite the rapid evolution of security products and services, understanding and mitigating risk remains the most critical business requirement for security professionals today. As a security leader, Weatheford said he finds that most companies do not know how and where they are spending money on security, and what is common to see is wasteful duplication of technology and services in situations where security leaders "haven't spent the money on the processes and the people."

Two areas, however, have taken center stage in the risk arena – security convergence and the supply chain. In this presentation, Mark Weatherford highlighted cyber-related convergence and supply chain events, identified various cyber threats and provided some insight into the things your company should be thinking about to mitigate threats in this space.

Key Takeaways:

- The physical and digital worlds are increasingly blurred, and supply chains must now focus on effectively converging. Both physical and information security are integral parts of a coherent risk management program.

> "We need more secure products, not more security products."
>
> *Mark Weatherford, Global Information Security Strategist, Booking Holdings*

- The top challenges for security convergence are differences in culture, language, adversaries, perception, experience and budget.
- Supply chain risk can best be managed by establishing a vendor risk management program; ensuring the security team is integrated into the procurement process, vendor assessments and vendor management; conducting regular briefings on the threat environment; and tracking the reporting and remediation of vulnerabilities.
- To build a more secure Internet of Things (IoT), we should focus on secure development, encryption, passwords, privacy and regulation.
- Businesses should examine the technology refresh cycle of physical security solutions and model the refresh cycle more like IT devices, which often have a faster technology refresh cycle than physical security devices.

View From the CISO's Office

Speakers:
George Finney, *Chief Information Security Officer (CISO), Southern Methodist University (SMU)*

Rick Grinnell, *Managing Partner, Glasswing Ventures*

Arve Kjoelen, *Deputy CISO, McAfee*

Tony Reinert, *Director of Information Security – Digital Home, Comcast Cable*

Mark Weatherford, *Global Information Security Strategist, Booking Holdings*

Summary:
As enterprises embark on digital transformation, leading organizations are emphasizing a converged risk management approach bringing new players to the decision-making table. Physical security solutions increasingly interact with critical data sources to deliver more value to an organization, so what are information security professionals interested in when interacting with their physical security counterparts and their partners? How can physical security provide value – and hence buy in – from these new decision makers with often bigger budgets? A distinguished panel of executives from the CISO's offices of leading organizations discussed these questions and more.

Key Takeaways:

- Bringing physical security and cybersecurity together under one office or department can help an organization make its security more comprehensive and effective.

- With technologies like artificial intelligence (AI), machine learning and the cloud, there are opportunities and benefits, but it's important to handle all this data responsibly and make rational, informed decisions when making moves to the cloud.
- IT leaders are seeking more cybersecurity in IoT and physical security products and looking for solutions that can be updated, solutions that are well tested and solutions with more compatibility.
- Converging logical and physical access and identity is an area with great promise, whether to solve fundamental problems of provisioning and unprovisioning or more advanced applications that link physical location with specific network access to help businesses better understand where employees are.
- There is a talent gap and a need for more talent in this space; companies must work to get more diversity into the talent pipeline, improve career paths and offerings to address turnover issues and explore ways that AI and other technologies can improve efficiency.

> "The longer you put off putting a focus on cybersecurity, the harder it's going to get."
>
> *Tony Reinert, Director of Information Security – Digital Home, Comcast Cable*

Integrating and Monetizing Cyber and Physical Security Offerings

Speaker:
Steven Mains, *CEO and Managing Partner, TechMIS LLC*

Summary:
Can security integrators monetize cybersecurity? To do so, they need to offer managed security services that provide long-term security for clients and a steady revenue stream for their integration business. To do this, integrators need to understand what threats companies face and know what products and services mitigate those threats. This discussion examined how cybersecurity offerings complement physical security and can be sold as managed security services with ongoing revenue, what cybersecurity products and services address current threats and how services can be bundled into managed security service contracts.

Key Takeaways:
- There is a cybersecurity equivalent to everything a physical security integrator includes in its portfolio (like access control, perimeter monitoring and fraud prevention); both sides of security are about maintaining customer reputation.
- Hackers evaluate the strength of various targets and go after the weakest ones; it is important to be stronger than those around you.
- There are three different cybersecurity monetization models for a security integrator: 1) providing a list of recommended vendors to potential clients, 2) integrating companies who are cybersecurity experts into the security sales and project team and 3) having full cybersecurity capabilities within the company. The first option is a broken model, and the third can be costly and difficult for most companies, so partnering with a cybersecurity company may be the most appealing from an investment, client and income stream perspective.

Dissecting the Attack – How Hackers Target and Compromise Products and Systems Just Like Yours

Speaker:
Valerie Thomas, *Executive Information Security Consultant, Securicon*

Summary:
Nearly every day, the headlines are full of breach announcements of major companies and organizations that leave us with many questions. How do these breaches happen? Why didn't anyone notice? Why does this keep happening? Could this happen to me? This session covered how attackers select, plan and attack their targets from start to finish with real-world scenarios and what a company can do to protect its reputation as a manufacturer or systems integrator.

Key Takeaways:
- Now that blended cyber and physical attacks are becoming more mainstream, physical security technology and the companies that create and deploy it are high-value targets for hackers.
- Individuals can better protect themselves by reviewing their resumes and LinkedIn profiles, considering using burner phone numbers or Google Voice for documents like resumes and social media, removing metadata from shared/uploaded documents and avoiding using professional email addresses for social media, job searching and conference registration.
- Companies should consider using dedicated

workstations for the access control environment and dedicated laptops for client equipment maintenance and educating staff on the dangers of USB device attacks, phishing and file-based attacks.

- Security companies should:
  - eliminate default passwords in equipment and software
  - test and retest products internally and by outside organizations
  - establish vulnerability tracking and reporting programs
  - know what third-party software is used in each device
  - create security resource centers for integrators and end users
  - update internal security awareness training programs and include cybersecurity in the development process.

Converged Security and the Law

Speaker:
Alexander Urbelis, *Partner, Blackstone Law Group*

Summary:
What can a hacker and a lawyer teach the physical security industry about the legal landscape of cybersecurity? We all know that costs and liabilities associated with cyber breaches are multiplying; however, there is a tremendous number of cybersecurity blind spots that threaten the industry and can rare their ugly heads in the near future. In this presentation, cyber-legal mind Alexander Urbelis took a microscope to some of the glaring legal ramifications that can impact the industry specifically and issues relating to the domain name system (DNS), intellectual property, nation state actors and privacy of information collected by security systems.

> "DNS enforcement has become a game of whack-a-mole."
>
> *Alexander Urbelis, Partner, Blackstone Law Group*

Key Takeaways:

- There are an increasing number of malicious attacks using malicious domain names and sub-domains; regulation of these domains is largely nonexistent.
- Other common attack types include hacking legitimate domains and diverting traffic to counterfeit sites, state-sponsored organizations impersonating HR functions and credential harvesting attacks.
- It's important to understand any exceptions to your cybersecurity insurance plan and what is and is not covered.
- When responding to serious cyber incidents, Urbelis recommends that outside counsel hire consultants and investigators (rather than being hired directly by the firm); this makes the work those contractors not discoverable in litigation due to legal privilege.

Building a NIST-Compliant Cybersecurity Program

Speaker:
Larry Wilson, *CISO, University of Massachusetts President's Office*

Summary:
Five years after its initial release, the National Institute of Standards and Technology (NIST) Cybersecurity Framework is still a gold-standard process for prioritized, flexible, repeatable, performance-based and cost-effective approach to managing cybersecurity risk at all levels in an organization. The framework is applicable to organizations of all sizes and sectors. This presentation addressed using the NIST Cybersecurity Framework for building a cybersecurity program that addresses today's cybersecurity landscape and cyber risks, providing attendees with assessments, executive score cards and a road map to remediate control gaps.

Key Takeaways:

- The NIST Cybersecurity Framework is a systematic process for identifying, assessing and managing cybersecurity risk; its core functions are to:
  1. identify (what assets need protection?)
  2. protect (what safeguards are available?)
  3. detect (what techniques identify incidents?)
  4. respond (what techniques contain impact?)
  5. recover (what techniques restore capabilities?)
- Using the framework as a cybersecurity risk management tool, an organization can determine activities that are most important to a critical service delivery and prioritize expenditures to maximize the impact of the investment.
- Continuous diagnostics and mitigation (CDM) helps organizations procure a set of tools that will provide cyber professionals with real-time analysis of their networks, assess risk and threats, mitigate and identify flaws at near network speed, create a smaller attack surface and decrease risk for operational networks, find weaknesses and vulnerabilities,

improve hardware and software asset management and vulnerability management, create dashboards to show network security and improve management and trust of people granted access to networks.

- In a NIST-compliant cybersecurity program, senior management is responsible for the cybersecurity strategy, workforce, governance and policy; risk management oversees the systems security plan, cyber risk assessment, plan of action and milestones and executive report; cybersecurity engineering is responsible for what and who are on the network, how the network and data are being protected and what is happening on the network; and cybersecurity operations is responsible for basic, foundational and organizational security controls.

Enterprise Technology Trends to Watch

Speakers:
Brandon Reich, *Senior Director of Surveillance Solutions, Pivot3*

David Stevens, *Chief Solutions Evangelist and Architect, HyTrust*

Summary:
Research firms forecast that video will produce 15.1 zettabytes of data annually – no other IoT application comes close to this rate of data production. This influx in data, as well as the growing adoption of video analytics and AI, propels video to be used in a wide variety of ways. These trends enhance video's value but also pose challenges, such as threats related to cybersecurity. This presentation explored how the latest innovations in IT enable users to better capture, store and protect data. It also highlighted how data has become today's "modern currency" and how deep learning enables you to pinpoint the exact data that is important to your business.

Key Takeaways:
- Video is leading the IoT revolution with more sophisticated technology, more use cases and moving to the data center.
- As IoT volume grows, demands on infrastructure and management complexity increase.
- A three-layer approach to security is recommended; layer 1 is about workload and data (where data lives, how it is transferred and key management), layer 2 involves authentication (e.g., multi-factor authentication, privileged access control and secondary approval) and layer 3 is environment hardening (e.g., information assurance, vulnerability assessments, automated security and compliance assessment, geofencing, encryption and data access audits).
- It is important to cover multiple stakeholders – infrastructure and operations and IT security and risk management – to become more competitive and drive business growth.

A Year of Frustration – a RASP Deployment Story

Speaker:
Troy Bowen, *Manager, Application Security, Verizon*

Summary:
For any organization that has attempted a runtime application self protection (RASP) deployment, you know the frustrations that come with getting C-level buy-in and customer engagement. This presentation walked through the ups and downs of a successful RASP deployment, including how to deal with delays, how to measure whether the deployment is actually working and how to integrate your RASP deployment with common security information and event management tools while consistently delivering added value to the business.

Key Takeaways:
- RASP is a security technology built or linked into applications or application runtime environments that can control application execution and detect and prevent real-time attacks like clickjacking, database access violation, insecure cookies or transport, unauthorized network activity and weak authentication, browser cache management or cryptography.
- Deploying RASP has a number of benefits, including that it gives developers time, moves beyond speculative security issues and allows visibility to be distributed to various security functions, like developers, management and the global security operations center.
- After a failed attempt at deploying RASP, Verizon succeeded by hiring a dedicated team including a project manager, manager and staff, attacking the problem and forcing teams to implement; it is important for management to consider how the deployment should be handled before starting.

You've Been Breached – What Happens Next?

Speakers:
Wayne Dean, *Vice President, McGriff Insurance Services*

Hannah Hoeflinger, *Professionals Lines Broker, INSUREtrust*

Summary:
Post-cyber breach, your next steps are critical to the recovery success or potential demise of your company. What do you do? Who do you call, and when? The time to create a data response plan is before an incident happens. During this session, Dean and Hoeflinger discussed the critical components that should be included in a cyber incident response plan to help protect you, your customers and your company from reputational and monetary damages.

> "Having an incident response plan is the #1 factor in quickly responding to a breach and avoiding losing a lot of money."
>
> *Wayne Dean, Vice President, McGriff Insurance Services*

Key Takeaways:

- The state of the cyber insurance market involves a race to keep up with sophisticated hacking activity, a race for innovative coverage, a large number of carriers with varying levels of experience and growing premiums for cyber-first carriers.
- The leading threats to data are employee mistakes, hackers, system of process malfunction, malicious insiders, temporary or contract workers, third-party service providers and lawful data request. Types of threats include nation states, organized crime, hacktivists and insiders.
- Having a full cybersecurity insurance policy provides a great deal of value other than just loss of data coverage; it helps drive the cost of a breach down and provides pre- and post-breach resources, vulnerability reports and upfront claims assistance.
- General liability policies have weak cyber coverage; cyber insurance covers things like privacy liability, network security, electronic data, breach of privacy and more.
- Incident response planning and risk transfer should include vendor risk management, becoming familiar with the legal counsel provided by cyber policies, involving board members in cybersecurity decisions, keeping high employee awareness and training standards, encouraging incident reporting, limiting sensitive data privilege, requiring authentication, knowing where sensitive data is, limiting aggregation, keeping up to date with state and international privacy laws and limiting adverse media and negative public/customer perception.

Convergence: It's More Than a Buzzword

Speakers:
Bill Eckard, *Director, Strategic Accounts, Verint Situational Intelligence Solutions*

Jeffrey Lewis, *Vice President, Marketing, Verint Situational Intelligence Solutions*

Summary:
In today's world, security is mission-critical and needs to be looked at holistically. The once predominantly physical security business is no longer enough to protect against an increasingly complex risk landscape. As today's threats and breaches frequently target an organization's IT infrastructure, it is paramount that businesses turn to a more unified and collaborative security strategy that incorporates both physical and cyber aspects. This requires convergence among the enterprise: cyber, IT and traditional security teams must unite to strengthen risk mitigation. In this session, Eckard and Lewis discussed how to efficiently combine cyber and physical security threat considerations and teams, develop a proactive risk management strategy to stay one step ahead and identify the importance of gathering intelligence from various sensors and sources to obtain increased levels of insight into threats and apply that information to physical security solutions.

Key Takeaways:

- Social media can be used for early warning intelligence, surfacing events that could be security incidents and monitoring live traffic for posts that meet criteria.
- Social media monitoring firms are still seeing lots of user data going public due to poor use of privacy controls by users on common social media platforms.
- Social media monitoring fuels a comprehensive, cohesive security strategy and feeds the larger physical security engines: situational awareness, video surveillance, facial recognition and dispatch and response.
- Integrators were encouraged to resell social media monitoring; identifying the right partner involves evaluating experience, breadth of portfolio, open architecture, cyber and physical expertise and commitment to customer success.

Gap Analysis: Configuring Your Microsoft Office 365/Azure Environment(s) for NIST 800-171 Compliance

Speakers:
Andrew Lanning, *Defense Industrial Base Sector Chief, InfraGard Hawaii Member Alliance*

David Stevens, *Managing Director, Kapu Technologies, LLC*

Summary:
Supply chain cybersecurity scrutiny is increasing across the entire critical infrastructure ecosystem, not just the Department of Defense. This presentation reviewed the common gaps found in subcontracting environments that use Microsoft Office 365 and/or Azure IT environments and included advice for configuring, monitoring, automating and reporting upon shared NIST 800-171 controls.

Key Takeaways:

- Companies that use Office 365 and Azure to process and store controlled unclassified information (CUI) must comply with the Federal Acquisition Regulation (FAR), managed by the U.S. Department of Homeland Security, NASA and the U.S. General Services Administration, and the Defense Federal Acquisition Regulation Supplement (DFARS), a supplement to the FAR that provides U.S. Department of Defense (DOD)-specific acquisition regulations DOD government acquisition officials and contractors must follow in procurement of goods and services.
- There are free tools that can be used to aid in compliance, or companies can use Federal Risk and Authorization Management Program-compliant cloud service providers.
- Confidentiality, integrity and availability are key to balancing business objectives.
- Satisfying requirements does not make a company secure; implementing and regularly auditing requirements creates a secure system.
- A company's organizational needs will guide it to choose the correct Office 365/Azure level of service to comply with DFARS/NIST.

Technologies Transforming Cyber-Physical Security

Speakers:
Min Kyriannis, *Associate, Cybersecurity, Jaros, Baum & Bolles*

Edward Lee, *Security and Trust Advisor, Google Cloud*

Jimmie Lee, *Head of Security Applications – Global Security, Facebook*

William P. Woods, *Senior Director – Security Intelligence, McAfee*

Summary:
Advanced cloud capabilities, AI, facial recognition analytics and quantum computing have all been mentioned in trade and general business press as the next big disruptors. But how quickly do implementers of security need to understand and weave these technologies in their solutions? In this session, technology evangelists from leading technology platform organizations discussed these technologies and others, including the security problems that they solve and the new attack surfaces and risk that they present.

Key Takeaways:

- As cybersecurity and physical security converge, one way to differentiate the two is considering what kind of asset you are trying to protect (e.g., people, places and reputation or a computer network).
- Even if the cyber and physical security programs are separate, bringing them together as much as possible (as McAfee did by housing them in a single security fusion center) can help companies provide more comprehensive, effective security.
- Cloud technology can allow benefits like central monitoring from anywhere and can be configured to allow a more secure environment for customers; however, it exposes companies to compliance concerns like GDPR and overall data protection.

> "If we continue to compartmentalize, the cyber risks will be far greater than if we do this as a fusion team."
>
> *Jimmie Lee, Head of Security Applications – Global Security, Facebook*

- Facial recognition, AI and biometrics have a lot of potential in terms of how they can play a role in physical security moving forward.
- Encryption of data should be a requirement, noted Facebook's Jimmie Lee. Google's Edward Lee reinforced that point, noting that in the Google cloud environment, encryption is the default, with everything encrypted at memory before being written to disks.
- Before investing in a new technology, it's important

to make sure your networks can support it and that it aligns with business goals and provides services and forward growth; additionally, companies should look at use cases and determine the most fiscally responsible solutions that will address their needs.

What Physical Security Can Learn From Cybersecurity

Speaker:
George Finney, *CISO, SMU*

Summary:
Whether their focus is on hackers or intruders, security teams struggle with the same issues and often compete for the same budget. Increasingly, law enforcement, chief security officers and CISOs are concerned with blended attacks that have physical intrusions in conjunction with or in support of cybersecurity breaches. This session explored the lessons learned from the CISO of SMU, which has integrated support for physical security technologies and cybersecurity on the same team. Five years later, the team has completed a campus-wide lockdown initiative, centralized support, increased response time, improved the student experience and helped to reduce crime on campus – all while hardening systems against hacking.

Key Takeaways:

- Physical security and cybersecurity teams have a lot of similarities; they both integrate complex ,technologies that operate behind the scenes, and they both must stay one step ahead.

> "You can't have cybersecurity without physical security, and you can't have physical security without cybersecurity."
>
> *George Finney, CISO, SMU*

- The 2012 selection of SMU as the location of the George W. Bush Presidential Library and Museum began a process of improving security across campus, including implementing thousands of surveillance cameras and card readers and a central real-time interface, all with the existing staff; partnering with an integrator was instrumental in carrying out this project efficiently and strategically.
- SMU's IT and police departments worked together to move the needle and reduce crime on campus.
- It's important to understand and address security blind spots, including the need for security team diversity, the human impact and the need to streamline tools, share information, collaborate and standardize.
- Organizations should create cultures of security through implementing programs like phishing awareness training, cybersecurity-themed escape rooms and other activities.

Four Big Questions: A Discussion of the Cyber-Physical Challenges Facing the Industry

Pillars of a Cybersecurity Hardening Guide

Speaker:
Adam Firestone, *Chief Engineering Officer, Secure Channels*

Key Takeaways:
Experts with conflicting messaging about password protocols can sometimes be outdated and frustrating; multi-factor authentication is the way to go beyond just passwords and biometrics (secure passwords, idiomatic recognition windows, picture password systems and combined tokens).

Solution ideas for default passwords include 1) decentralizing concepts for password use), 2) using InterPlanetary File System (IPSF) using a distributed hashtag rule to decentralize everything, 3) using DNS servers to use IPSF as a standard and 4) using embedded firmware going forward.

Privacy in the Age of Connected Devices

Speaker:
Michael Knight, *Global Chief Technology Officer, Dell Technologies*

Key Takeaways:

- Four key privacy concerns are:
  - 1) personally identifiable information and new data privacy laws creating challenges,
  - 2) a need for encryption of data in the industry,
  - 3) the IoT effect on privacy and
  - 4) lack of control over data
- Companies need an opinion on what is right, what must change and how we go forward.
- There is a need for open standards or an industry framework on managing data and privacy.
- It's important to educate the next generation on privacy before it's too late.

Gap Analysis: How the Security Industry Should Address Cybersecurity

Speaker:
Gary Hoffner, *Vice President, PSLA Security*

Key Takeaways:
The most pressing needs for industry guidance on cybersecurity are 1) standards, which are crucial, 2) more industry-driven training and certifications, 3) guidance and training for business leaders and 4) definition of skills gaps and compensation packages.

To address the information security/cybersecurity talent shortage, companies must develop cultures conducive to the cybersecurity space, develop cyber governance plans within their own enterprises, embrace higher compensation plans for cybersecurity employees and begin training the existing workforce on cybersecurity.

Show Me the Money: Considerations for Monetizing Cybersecurity as an Integrator

Speaker:
Bill Bozeman, *CEO, PSA Security Network*

Key Takeaways:
- If you are not going to get into the cybersecurity business, you must, at a bare minimum, have cybersecurity insurance.
- Going into business with a solid cybersecurity partner is a smart decision and a great way to monetize as an integrator.
- Integrators are starting to make the investment in cybersecurity now; several years from now, firms will not have a choice but to have cyber capabilities because customers will not want to do business with firms that don't have cybersecurity capabilities.
- Moving to a recurring revenue model is great for day-to-day operations, and your recurring revenue is also key to your exit valuation.

The Cloud and You: Cybersecurity in the Cloud

Speaker:
Chris Peckham, *Chief Operating Officer, Building Intelligence Inc.*

Summary:
The cloud has revolutionized the scale and security of physical security operations, reducing maintenance and provisioning time and redirecting those efforts to the actual practice of security; however, even with the major cloud service providers ramping up security and implementing world-class cybersecurity procedures, these back-end practices do not always translate to security on endpoint applications, as standards and APIs must be configured securely by customers. This session took attendees through the recommended on-premises procedures of deploying a security application securely on the major cloud services.

Key Takeaways:
- There are three models for cloud provisioning: user self-provisioning (simple, customer pays for services by card), dynamic (scalable, pay-per-use services) and advanced (formal, flat-fee or monthly billing contracts for defined services).
- Cloud environments minimize costs because capacity is provisioned based on average use rather than peak use.
- Right-sizing is an ongoing process within an organization: performance and capacity requirements can change over time, and organizations should have schedules, monitor costs and tag instances to know what is running.
- In managing infrastructure, it is recommended to use a bastion host or a jump server to help protect the system, leverage cloud monitoring and implement multi-factor authentication.
- Many vendors are now supporting applications in the cloud.

Selling Deterrence by Denial: Security Products, Hard Targets and Protecting Your Customers' Crown Jewels

Speaker:
Adam Firestone, *Chief Engineering Officer, Secure Channels, Inc.*

Summary:
Over the past decade, hundreds of millions, if not billions, of dollars of valuable data and the future opportunity it embodies have been stolen from American industry. Despite huge investments in cybersecurity, breaches and data thefts continue to happen on what seems to be an exponentially increasing basis. The uncomfortable truth about that investment, however, is that it has focused on failed methodologies or closing the barn door after the horse has bolted. This session explored solutions and exemplary products that implement "deterrence by denial," a cyber defense strategy that assumes an attacker will be successful in pene-

trating the perimeter but removes financial motivation to do so by rendering the ultimate targets of the attack, industrial information and intellectual property, useless even if successfully stolen.

Key Takeaways:

- The workforce is changing, with a growing number of knowledge workers and more distributed, virtualized and/or outsourced workforces.
- Most value is created at the edge, but edge device security has not kept pace with value virtualization or the threat.
- Attacks are economically motivated and all about data and return on investment; this shifts the definition of security to making attacks a risky investment for hackers.
- Companies can make themselves less appealing to attackers through deterrence by denial: making data unreadable and unchangeable by unauthorized users and making it indestructible and/or durable.
- There are software products that provide deterrence by denial capabilities, a growing market for them and opportunity to profit, but it's important to make sure your customer and organization are ready and choose appropriate products and partners.

Defending Today's Hybrid IT Environments With Managed Detection and Response

Speaker:
Eldon Sprickerhoff, *Founder and Chief Innovation Officer, eSentire*

Summary:
Modern-day cybersecurity threats require close monitoring and effective response; however, as data expands from on-premises to the cloud – or somewhere in between – new blind spots are emerging. Threat actors are taking advantage and accomplishing their objectives faster than ever, and traditional SIEMs have proven to be ineffective at defending against new cyber-attacks and risks. Today's hybrid IT environment therefore needs an additional spectrum of visibility with integrated detection and response capabilities to catch the most elusive of threat actors. This presentation addressed the evolution of data security, including why traditional SIEMs are falling short, why hybrid IT environments require an additional spectrum of visibility, the level of risk associated with differing levels of visibility and the effects the addition and removal of each data signal can have upon a risk profile.

Key Takeaways:

- Today, the attack surface is expanding; threat actors are motivated, creative, sophisticated and well funded; and the cybercrime economy is well established. Attacks are opportunistic, industry focused and targeted.
- Rapid detection limits costs – the more quickly you can respond, the less damage there is to company reputation, operations and business.
- Having a distributed IT environment (leveraging machine learning, system logs, cloud services, endpoints and network) means full threat visibility and integrated response.
- Using technology can help reduce thousands of signals to a few key threats for human investigation.

Presented by

ISC INTERNATIONAL SECURITY CONFERENCE & EXPOSITION

PSA SECURITY NETWORK

SIA SECURITY INDUSTRY ASSOCIATION