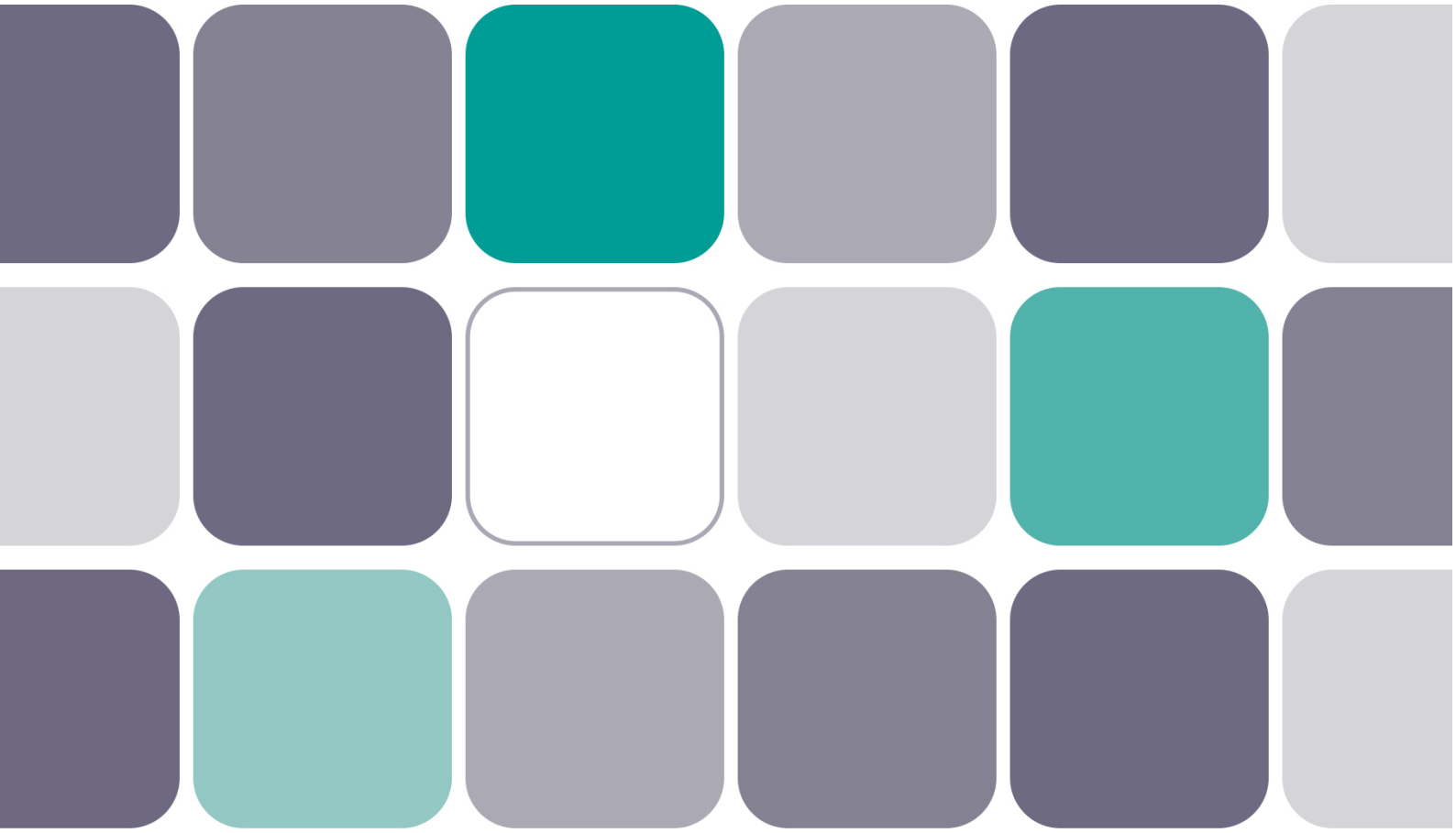
VOLUME ONE
NUMBER ONE
SUMMER 2017

ISSN: 2398-5100

Cyber Security

A Peer-Reviewed Journal



Multi-vector threats and the argument for greater convergence

Received: 10th February, 2017

Ron Chandler

serves as Vice-President for the Guidepost Solutions Security and Technology Consulting group specialising in Enterprise Solutions, where he is responsible for all service segments regarding the implementation of cybersecurity, global master planning/command and control programmes (GSOC) and managed security services programmes either as standalone service offerings or as an integrated suite of solutions for Guidepost's clients.

Guidepost Solutions LLC, 2800 North Dallas Parkway, Suite 350, Plano, TX 75093 USA
Tel: +1 469.568.0637; E-mail: rchandler@guidepostsolutions.com

Brent Hambly

is the Director of Security Assessments and Strategy for Revolutionary Security. Brent has over ten years' experience leading assessments, enterprise IT and software-intensive programmes, cyber and physical biometrics credentialing programmes and security awareness programmes. Brent specialises in analysing and advancing security programmes through baselining, identifying improvement opportunities and assisting organisations in achieving defensible postures. Brent holds a Bachelor of Science in Management Information Systems from LeMoyne College and a Master of Science in Technical Management from Rensselaer Polytechnic Institute. Brent also holds GICSP, CEH, Security+, and Network+ industry certifications.

Revolutionary Security, LLC, 350 Sentry Parkway, Bldg. 610, Blue Bell, PA 19422, USA
Tel: +1 267-664-4200; E-mail: brent.hambly@rev-sec.com

Jason Holcomb

is the Director of Industrial Control Systems Security for Revolutionary Security. Jason has been actively involved in helping secure SCADA, DCS and other operations technology (OT) for over 15 years, with experience spanning the utility, oil and gas, chemical and manufacturing industries. Jason leads both technical assessments and strategic consulting engagements, helping clients understand their cybersecurity posture and prioritise investments for improvement. He has created and executed new service offerings and assessment techniques, led multi-year projects to perform ICS vulnerability assessments across the globe, and performed research for commercial enterprises and Department of Energy projects. Jason earned a BS in Computer Science from Evangel University and an MA in Computer Resources and Information Management from Webster University. He holds multiple certifications including CEH, CISSP and BOSIET.

Revolutionary Security, LLC, 350 Sentry Parkway, Bldg. 610, Blue Bell, PA 19422, USA
Tel: +1 267-664-4200; E-mail: jason.holcomb@rev-sec.com

George Ressopoulos

is the Director of Enterprise Security Transformation for Revolutionary Security. George has over 15 years' IT and cybersecurity experience. He has extensive experience leading cyber defence transformations, including: Red Team, Blue Team, Corporate Security Assessment Team, Computer Incident Response Team (CIRT), Vulnerability Remediation Team, and Enterprise User Awareness and Education Team. George specialises in designing and transforming cybersecurity defence organisations aligned with industry recognised frameworks, such as the NIST Cybersecurity Framework. George holds a Bachelor of Science in Management Information Systems from the University of Central Florida and a Master of Science in Business and Organizational Security Management from Webster University.

Revolutionary Security, LLC, 350 Sentry Parkway, Bldg. 610, Blue Bell, PA 19422, USA
Tel: +1 267-664-4200; E-mail: George.ressopoulos@rev-sec.com

Matthew Wharton
serves as president for the Guidepost Solutions Security and Technology Consulting group and oversees its core services, including cybersecurity, system design and project management, global command and control centres, security assessments and managed services. He is a career security professional with more than 30 years' experience leading security consulting and integration firms.

Guidepost Solutions, LLC, 2800 North Dallas Parkway, Suite 350, Plano, TX 75093 USA
Tel: +1 469.568.0615; E-mail: mwharton@guidepostsolutions.com

Abstract Due to technological innovations and priorities to manage risk at the enterprise level, convergence is occurring between physical and information security functions, responsibilities and missions. In order to adapt to this evolving security environment and protect the organisation from multi-vector threats, information technology (IT), operational technology (OT), and physical security groups must develop trust, enhance communications and information sharing, and engage in cross-domain adaption. As the convergence occurs, organisations are experiencing more multi-vector threats from diverse actors. One area with a high potential for convergence is the security operations centre (SOC). If done properly, the combined joint security operations centre (JSOC) is the most effective way to manage security risks. This paper will address how organisations can best integrate these disparate functions, situations where this cohesion is most effective, and best practices to increase the effectiveness of this integration.

KEYWORDS: convergence, cybersecurity, joint security operations centre (JSOC), operational technology (OT), physical security, security operations centre (SOC)

MULTI-VECTOR THREAT

Cyberthreats have traditionally been associated with an adversary remotely attacking a corporation's networks and resources. While this may be true in many cases, the potential for a physical security breach to permit logical network and data compromise is often underestimated. While physical security has technical and administrative elements, it is often overlooked because most organisations focus on technology-oriented security countermeasures to prevent intrusions.[1]

Successful physical-to-logical attacks often result in long-term persistent logical intrusions with potential catastrophic impacts. Due to risks associated with this type of intrusion, these adversaries are often sophisticated, well-funded and committed to the attack. Defending large and targeted corporations requires a commitment to a holistic cyber defence programme, including physical and logical threat coverage. A multi-vector threat defence programme explores opportunities to enhance and optimise existing capabilities and maximise security investments. Where applicable, organisations should strive to go beyond alignment to industry best practices and compliance. They should take action to enable an advanced threat defence capability, resiliency and sustainability.

MULTI-VECTOR ATTACKS

Companies have historically experienced losses due to data breaches or denial of service that have come from the traditional threat vector of breaches in the logical protection layer via targeted hacking, advanced persistent threat, phishing, malware, and other methods that logical countermeasures mitigate.

Threats are emerging that involve either a simple instance of the scenarios above or

a combination of these scenarios in a multi-level attack:

- Compromise/sharing of contractor credentials
- Physical access to logical assets by unauthorised personnel
- Utilisation of remote logical credentials for accessing restricted assets by individuals who are not in proximity to the asset.

These multi-vector threat scenarios cut across the countermeasures that are traditionally implemented by either the physical or logical security mitigation toolkit.

As cyber defences improve, the ability to deliver malware and execute attack objectives against certain protected network enclaves will become more difficult. For environments where it is challenging and costly to logically deliver a cyberattack, physical delivery becomes a more economical choice; that is, attackers wishing to conduct malicious operations are more likely to use a physical means to commence the attack process. This could take many forms, including portable media, direct human–machine interaction via unauthorised entry into a physical security zone, or simply gaining access to a logical network connection by targeting cables or network jacks and adding an out-of-band wireless or internet-connected access point. The authors have experience performing on-location penetration testing for a high number of diverse enterprises. This experience has shown that attackers can gain network administrative privileges, undetected and without any prior credentials, on most networks within a few days of gaining physical access to an internal network drop.

Attackers who are targeting a specific entity are more likely to use multi-vector attacks as organisations concentrate on either information or physical security controls. The authors witnessed a microcosm of this situation involving an organisation which engaged a third party to perform penetration testing services over the span of multiple years. As the organisation increased its logical security capabilities, the attackers turned to physical access to install compromised hardware, such as key loggers and network access tools. As a consequence, the organisation's logical and physical security teams became more intertwined to the point where security personnel on site were able to track the attackers via surveillance cameras and send out 'Be On the Lookout' (BOLO) notices to site staff.

Each of these examples represents a multi-vector security threat that can only be defended through a combination of physical and information security controls. A common multi-vector attack involves leaving a portable media device in a target location to entice a user to connect the media to a computer, unleashing malware planted on the device. This is sometimes referred to as a USB drop. While the physical aspect of the attack is passive, it has been a proven means for malware delivery. Perhaps the most famous example of this occurred in Operation Buckshot Yankee. In 2008, the National Security Agency (NSA) discovered malware on classified systems. Upon further investigation, they determined that the initial malware infection and subsequent replication of the malware spread via a USB flash drive.[2] These devices are, of course, now banned from most federal computers in the US.

Multi-vector threats that emerge from within an organisation are frequently cited as a top concern for security professionals due to the higher level of harm that insiders can cause.[3] Insider threats can be intentional or negligent in nature, necessitating tailored detection and distinct preventative mitigations from both the physical and logical domains. This can include monitoring of the individual's activity on the company premises, review of files accessed and modified by the individual, inspection of when the person arrived and left the office, etc. Table 1 demonstrates precursors and outcomes from insider threat activity.

Table 1: Precursors and outcomes from insider threat

Precursors	Outcomes
Unauthorised or abnormal network activity	Information/device theft
Decline in employee performance	Unauthorised data manipulation
Indications of financial difficulty	Network attacks
Unauthorised physical access	Operational disruption
Tailgating	Facility destruction
Implantation of rogue devices	Industrial espionage

While most organisations would be well-served to consider insider threat, risk factors associated with insider threat should be viewed holistically as a behavioural profile. Technology solutions now have a more granular, integrated view of threats to organisations. These tools are broadly categorised as User and Entity Behavioural Analytics.[4] Technologies can, however, vary from network activity-focused monitoring and alerting to comprehensive behavioural profiling. Behavioural trending can include:

- Safety controls status
- Control system user access and activity
- Control system status and configuration changes
- Network operational status
- Security technology alerts

APPLICABILITY

Multi-vector threat defences vary across organisations based on function, size, geographical distribution, and criticality. Determined attackers can leverage both physical and logical pathways to achieve goals. These goals might be to steal data, compromise systems, gather intelligence, or even cause kinetic actions. The Stuxnet worm and subsequent disruption at the Natanz nuclear facility is a prime example of the complexity of the multi-vector threat environment. The perpetuator of the attack first had to compromise the physical systems to introduce the multi-stage malware that ultimately affected the control logic in Siemens programmable logic controllers (PLCs) and caused the nuclear centrifuges to operate beyond their capacity. Most experts agree that Stuxnet was the work of sophisticated, state-level attackers.

While many organisations are unlikely to face this level of sophistication, an attack does not have to be highly complex to exemplify the multi-vector threat environment. The concept of breaching physical security, such as manipulating weak locks, tailgating or shimming doors on server rooms, is a common, but often overlooked, vulnerability. Just as Stuxnet was a logical attack with physical consequences, physical break-ins on server rooms and datacentres can lead to information security consequences. For instance, in 2015, an attacker broke into a server room at a philanthropic organisation, Plan UK, and stole five servers containing personally identifiable information (PII). While the reason for taking the servers is unknown, this physical act caused an information compromise. Attackers generally look for the path of least resistance; that path might be a logical gateway or a front door.

CURRENT APPROACH

The current approach to defending a large enterprise and its resources is often decentralised and disjointed. This is due to the fact that organisations do not have full visibility into their complete risk positions. This spans across both functional and technical components and often includes blurred communication rhythms, limited

integration, and decentralised systems and platforms. In large organisations, the evolution to a common access card has intuitively driven integration and alignment between physical and logical security systems. Where this evolution is lacking, however, is the integration of system log sources and physical access data for the detection of multi-vector attacks.

In most cases, functional integration across physical and logical security teams has been limited or non-existent. The security operations centre (SOC) defending the organisation's physical assets is isolated and distinct from the SOC protecting its information resources. Executive leadership often lacks the awareness necessary to understand the importance of holistically defending a large organisation and its resources. Treating physical and logical security threats as disparate or independent entry vectors impedes the ability of organisations to adapt their defensive model for a multi-vector threat approach. Physical-to-logical convergence is not a next generation concept. Organisations should embrace the opportunity to improve communications, enhance cross-functional collaboration, and improve threat detection and response capabilities.

CONVERGENCE EXAMPLES

Within the financial services sector, some companies have implemented a truly converged SOC environment. In this arrangement, professional analysts and operators are co-located within a facility that provides tactical applications for the management and mitigation of specific threats while concurrently providing strategic information-sharing. This strategic vision allows for global situational awareness of emerging threats and allows the SOC staff to determine if the threats are logical, physical, or multi-vector. Practitioners use collaborative tools to identify and track the vector for each threat and specific communication, mitigation, and escalation protocols used by the SOC staff in managing the threat from alert to resolution.

The counterbalance to this fully converged environment exists in many major corporations today. The organisation defines a singular mission to provide monitoring and administration over a specific security technology platform upon the completion of its installation. The SOC is provisioned to provide this function with an acute focus on handling information output from this singular structure. This focus on a single information feed may seem to provide an extra management layer over a major capital investment. The threat landscape, however, is so broad and diverse that organisations often cannot glean actionable intelligence, sufficient to manage corporate risks, via a single source of information.

Some companies are making the gradual transition from singular focus (ie monitoring physical access control platforms) to a more strategic approach by integrating global risk platforms and increasing visibility into the IT environment. Taking these initial steps can be productive as they move the security function to a more converged model. This process should commence with a strategic plan for convergence, noting critical functions. Starting from this narrow focus and gradually including one *ad hoc* monitoring or functional model at a time exposes the organisation to the risk that critical functions may be missed in the process. Developing an overarching end-state vision first and then adding support modules to achieve this goal provides a higher likelihood of success.

DRIVING FACTOR FOR CONVERGENCE

Cybersecurity threats are among the top three issues facing corporate boards.[5] These threats continue to drive investment in cybersecurity defence, specifically the IT security budget. A multi-threat, multi-vector

security programme requires an extension of that budget integration to improve physical defences from a logical compromise. Both identity and access management provisioning and the movement to a 'one access badge' solution have driven recent advancements in physical-to-logical convergence. Capitalising on this efficiency is critical in advancing security defences and converging physical and logical information security.

BEST PRACTICES FOR PARTNERING AND UNIFICATION

Information security leaders and practitioners know that technology by itself is insufficient to address the varied risks threatening organisations. Entities must apply a defence-in-depth strategy across three stages: threat prevention, incident detection, and incident response.[6] At the core of this strategy is an executive commitment to promoting a transparent culture of 'Security First'. This means that the organisation embraces both information and physical security as key elements in its risk management programme, and that security is a primary factor which influences the strategic and tactical decisions made by leadership.

When creating a physical-to-logical convergence programme, security leaders should first develop a concept of operations (ConOps) to clearly define the approach, goals and specific integration benefits for the organisation. ConOps should include the development or enhancement of a corporate incident response plan (CIRP). The CIRP should serve as the consolidated response procedures across organisational functions in the event of a large-scale cyber incident.

Once the ConOps is established, the developers should conduct an internal maturity assessment and identify the current state of physical and logical security integration. This will provide a mechanism to measure future growth, advancement, and identify specific areas on which to focus. At this point, the enriched data from the ConOps and internal assessment should provide the foundational information to plan, budget and execute a physical-to-logical security convergence project.

An organisation's approach to convergence can be fraught with significant challenges if proper planning and objective programme management are not adhered to throughout each phase of convergence. The overall goal of the converged platform is to enhance an enterprise's ability to identify, mitigate, or lessen the impact of multi-vector threats. For this reason, organisations must revisit their risk management process and matrix. This helps to identify the potential threats to the organisation within the context of the converged model. The risk management process often already exists and is reviewed annually or when the entity encounters major changes or incidents. The key is to use the existing risk matrix unique to the organisation and to take into account all tangible and intangible assets that can be associated with these converged risks.

Once the organisation identifies these assets, it can proceed with the outcome resulting in an extended set of collaborative controls, which can be applied to each asset or group of assets. This takes into account the multi-vector information identified during the risk-modelling phase. Once the organisation develops these collaborative controls, the technical, procedural, and operational implementation of the converged SOC commences. The organisation can then define the programme roadmap and implementation per the system development life cycle (SDLC).

Organisations should carefully consider the risk management process and each business line stakeholder. This visibility can support a better understanding of risk prioritisation for the overall enterprise. Lack of stakeholder participation during the risk identification or risk assessment modelling exercises will likely result in suboptimal controls with minimised effectiveness to the overall risk management goals.

FUNCTIONAL AND TECHNICAL BEST PRACTICES

Executive leadership support, advocacy, and empowerment is crucial to effectively transform and sustain an integrated, multi-vector threat defence programme. The top-down promoting the bottom-up approach helps advance the overarching goal, particularly if it is fostered first by the organisation's top advocates. Physical and logical security functions have traditionally been an organisational divide.

Leadership support

The executive leadership is responsible for bridging this divide. Ensuring the alignment among the CSO, CISO, and other executive leaders makes the collective management for the multi-vector threat programme possible. Organisations must seek to establish transparent, intuitive lines of communication, and infuse physical and logical security during daily operations. Effective crisis management requires establishing escalation thresholds and policies in addition to developing an inclusive decision matrix outlining decision authority based on incident scenarios.

Organisations must also establish key relationships across organisational lines and hold leaders accountable for promoting collaboration across teams. A number of options exist for how to do this. For instance, organisations can explore opportunities to host regularly scheduled joint threat status and reporting briefings. Organisations can also consider some rotational opportunities to intersperse physical and logical security staff.

Testing and awareness

As organisations begin to converge, they should consider targeted user awareness and training initiatives on both physical and logical security areas. These can also manifest in dual training and workshops to further reinforce the 'Security First' approach and consider convergence when addressing security concerns such as unauthorised removable media, supply chain integrity and unauthorised system access.

In this regard, the most important component in establishing an effective, agile, and sustainable multi-threat defence programme is testing it in simulated multi-vector attacks. Testing should include covert and overt activities to educate, prepare, and evaluate physical defence and logical detection mechanisms. Collaborative tabletop exercises and the evaluation of the CIRP on the connection between physical intrusion and advanced persistent threat scenarios can further elevate this endeavour.

Organisations should evaluate their defences with covert physical penetration testing designed to bypass physical controls and execute on a predefined physical-to-logical attack plan. If a team of undercover physical testers is able to attain access to the facility, can they access the server room? Can they plant a USB device in a production server? These are all considerations when testing the live defences of physical and logical security capabilities and areas to increase the awareness of the user community. While the results of testing should identify gaps in physical and logical defences, organisations should not use these results for punitive purposes. The intent is continued improvement.

Data integration

Technical best practices combine physical security control systems with cyber monitoring and defence capabilities enriched by big data analytics and anomaly-based detections. These technologies store large datasets in an environment capable of efficiently querying, correlating, and joining disparate information. The first

step in exploring technical integration is identifying common technologies, platforms, and technical gaps. Physical security control systems are typically decentralised and often require integration to collect common and consistent log information to security correction technologies, such as security information and event management (SIEM) or data analytics platforms.

Identifying log sources is important, as the valuable content within these logs provides physical security access data to correlate with logical datasets. This expands beyond the physical access control systems and could include log sources derived from travel recording systems, employee attribute metadata (Active Directory), and insider threat programme data. For example, organisations can develop anomaly-based rules to identify when an employee is on international business travel and if, at any time during that travel, her physical credentials are used to access a domestic facility. Collecting a trending of log sources can also provide criteria to detect an anomaly and conduct a joint physical and logical security investigation. For example, if a system administrator is regularly accessing the facility and server room during non-standard shift hours, physical and logical teams can jointly monitor network traffic and observe unauthorised removable media usage.

Another area of consideration is the convergence of physical and logical security intelligence. Geopolitical threats coupled with traditional cyberthreat intelligence provide organisations with both regional threat visibility and opportunities to benefit both logical and physical security capabilities. Similar to functional best practices, technical capabilities require continuous improvement efforts. As threats continue to evolve and adapt to defensive countermeasures, operating an agile multi-vector threat defence programme can protect organisations from high severity impacts.

ADAPTING TO MULTI-VECTOR THREATS

Critical to converged security operations is planning and preparing for large-scale incidents within a multi-disciplinary organisation. Combining physical and logical threats in the form of tabletop exercises is a best practice for enhancing cross-functional awareness and improving collaboration among the IT, OT, and physical security practices. When scoping these scenarios, organisations should consider the most likely vector for adversaries to crossover from physical to logical or vice versa. Aligning these scenarios with specific industry and company threat profiles enables organisations to extract maximum value from the exercises.

Since 2010, the North American Electric Reliability Corporation (NERC) has invited large electric utilities to conduct bi-annual tabletop exercises simulating cyber/physical attacks on the electric grid.[7] In 2015, GridEx III involved over 4,400 participants from 364 organisations in the US, Canada, and Mexico. While these exercises are encouraging signs of broad collaboration in defending national infrastructure, they also exemplify methods of how to yield the most value from simulations, namely accurate scoping, detailed planning, tight coordination, realistic execution, and actionable lessons learned. Several security vendors facilitate tabletop exercises as a service to assist organisations in gaining deep insights into the varied and high-impact effects of cyber/physical incidents. The intent is to define and prioritise the mitigation actions that maximise value.

JSOC FUNCTION COMMONALITY AND DISPARITY

At a conceptual level, physical, OT, and IT security operation centres have a common mission: to protect the enterprise. In addition, they operate at a comparable

cadence, and they perform similar activities. For instance, the threat-monitoring aspect of security operations yields significant commonality in the imperative to acknowledge and triage potential physical and logical threats in a timely fashion. Likewise, the investigative aspect of modern IT, OT, and physical security operations is rooted in the discipline of forensic science. Whether analysing a cybersecurity breach, reviewing the firmware on a specialised PLC, or conducting a personnel investigation, the pursuit of evidence-based outcomes is central to all. To that end, all security operational practices share a common analytical approach and mindset to combatting threats across multiple domains.

Cyber-focused SOCs typically commence with a focus on alerts received from technology solutions deployed with vendor-recommended default configurations across the enterprise. Cybersecurity analysts must then identify which alerts are of relevance during a process of technology tuning. A crucial aspect of the tuning process is the delicate means of reducing false positives without removing valid threats from view.

Physical SOCs also go through the process of tuning their technology to reduce false positives in accordance with vendor specifications. The occurrence of false positives for physical security technology often derives from faulty sensors or negligent human actions (eg an alarm resulting from a propped-open door). This is opposed to the overly broad rulesets encountered by cyber SOCs (eg noisy combinatorial logic within a SIEM). Sensors can include a collection of diverse devices:

- Automated barriers and bollards
- Building management systems
- CCTV cameras
- Fire detection systems
- Intercoms
- GIS mapping systems

Taking a closer look at threat-monitoring across IT, OT, and physical security yields some interesting parallels. While the devices, protocols, signals, and data monitored within each of the environments are diverse, considerable similarities exists between the protective and detective controls and infrastructure supporting the JSOC. Detection and prevention technologies include:

- Data destruction, encryption and exfiltration
- Application and database security
- Cloud infrastructure and services security
- Account privilege escalation and lateral movement
- Network device configuration changes
- SIEM threat and vulnerability management
- Identity and access management

In addition, the complexity of security technology architecture frequency of updates poses a challenge to all large enterprises. The consolidation of effort can achieve economies of scale through centralised deployment, operation, and maintenance of the organisation's security infrastructure.

Despite a common mission and similar operational concepts, the threats faced by physical security teams and cybersecurity teams are fundamentally different. Physical

Table 2: Sample list of security monitoring aspects and enabling processes

IT	OT	Physical
System compromises (server, host, mobile device)	Process integrity (eg parameters out of set point range/limit)	Physical access control systems
Network attack and intrusion sensors	Process state	Perimeter and facility intrusion detection
Malware detection		

incidents often involve threats to human life or well-being, whereas information security incidents rarely result in kinetic damage. Cyber incidents have the propensity, however, to spread rapidly and cause distributed effects. On the contrary, physical security incidents are generally confined to a specific geographical region or site. It is for these reasons that OT attacks can be particularly destructive. They combine the kinetic impact of a physical incident with the distributed and scalable elements that are common to information security incidents.

Cyberthreat actors are continually developing and proliferating malware variants (eclipsing 500,000 samples per month as of 24th January, 2017).[8] Physical attack vectors, although enhanced through recent technology advancements, remain largely unchanged. These disparities produce contradicting operational views; therefore, organisations must carefully scope and design the detection and response foci of security functions both in terms of operational procedures as well as the physical JSOC environment.

BUILDING A COLLABORATIVE JSOC CULTURE

Organisations should strive to establish a culture of 'Security First' with inclusion of multi-vector threats and their potential impacts. Achieving a diligent state of multi-vector security does not necessarily require the investment to build a JSOC or make drastic organisational changes. It does, however, require a commitment to continuous improvement.

When integrating IT, OT, and physical security functions into a common JSOC operating model, first prioritise each of the functions against the threat impact severity and probability. The goal is to concentrate on the most critical functions that need to be integrated first, such as security event and intelligence feeds which can fuse for added situational awareness. Organisations can then shift focus to more advanced functions, such as automation of JSOC workflows. Functional integration requires interoperable system architectures across IT, OT, and physical security domains, including:

- Timely threat and vulnerability data source integration and analysis
- Event detection filtering and analysis
- Advanced threat detection
- Cross-domain correlation
- Guided forensics
- Workflow integration and enhancement
- Integrated response and remediation[9]

Cultural convergence between physical and logical security programmes is primarily driven by the composition of staff and their prior experience. Physical security analysts typically join the SOC with backgrounds in law enforcement or guard services, whereas cybersecurity analysts come predominantly from technology-related fields, such as computer science or IT administration. The inherent differences in perspectives create contrasting views on the threat landscape and can only be considered complementary when those perspectives are merged through clear communications. The trend toward geographical dispersal and the 'follow-the-sun' operational model further complicates the challenge of integrating the culture of the JSOC. Even simple concepts, such as the difference between an 'operator' and an 'analyst', can be obscured as organisations conjoin and cooperate. Establishing on-going rhythms of communication at appropriate intervals for each of the teams will ensure that semantics do not impede the integrated security mission.

Cultures are beginning to converge, with physical security analysts increasingly reliant on sophisticated technology solutions to enhance and expand their monitoring and investigative capabilities, and cybersecurity analysts gradually shifting their focus from technical indicators of compromise

to the human motivations behind cyber intrusions.[10] The cultural differences and credentials of physical and cybersecurity analysts will remain, and this diversity of perspective is both a positive for the JSOC's operations and a point of divergence whose recognition benefits mission success for each respective team.

JSOC BEST PRACTICES

The missions and objectives of JSOCs are as diverse as the companies where they are implemented and the specific markets that they serve. This diversity drives specific use cases and workflows that are unique to the threat and regulatory challenges within these sectors. Awareness of global events is one of the most significant activities for any business. The mission for a SOC is to act as the company's eyes and ears and to broadcast alerts regarding any critical activity that could create disruptions for the safety and welfare of employees, remote assignments, clients, and normal business activity. One of the most commonly used models to help categorise, act, and respond to such multi-vector environments is the US Joint Directors of Laboratories (JDL) model.[11] Alerts, events and escalations resulting from the triggering of these controls are predestined to be either auto-mitigated (if possible) or are escalated to a higher analytical tier for deeper analysis.

These collaboration controls are part of the mission-specific functions implemented for consumption within the SOC operations model. The mission-critical functions encompass in-context signal data, log information, workflow analysis, analytics, and human-to-computer interaction.

The best practices that are present across all organisations are colocation, collaboration, and communication. Colocation simply means that both information and physical security professionals share a common operating environment. The ideal environment would be a single facility where analysts and operators from both disciplines would reside and perform their work duties in adjacent workspaces. This set-up cannot always be accomplished in a corporate environment where the departments' centres of excellence are often not in the same geographic location or where analysts are dispersed across a global footprint.

If physical colocation cannot be achieved, a virtual solution should be provisioned that allows all SOC personnel to share their work tools and skill sets in a similar information-sharing and incident management architecture. Collaboration involves the instant ability for an operator or analyst to 'bounce-off' information to their peers in a one-click fashion. This creates instant fusion between information and physical security practitioners and breaks down silos of information and workflow. Organisations should be able to identify threats as physical, information, or joint within moments of their inception. Analysts should then follow specific tracks through to resolution based upon their classification.

The SOC is, at its core, a communications centre, so the culmination of all tools and procedures is the communications protocols established to disseminate information within the centre. The centre also distributes this information to appropriate decision makers and determines the level of escalation for actions to follow the subject incident and then broadcast this information to the proper audience to take action in the field. These communications protocols govern the inception of an event. Effective SOC communication also manages the entire life cycle of an incident from its inception to dispatch.

CONCLUSION

As companies seek to approach risk from an enterprise perspective and as technology draws IT, OT, and physical security closer, convergence will continue. The JSOC provides a proactive structure to address key threats to the organisation. Insider threat

is a prime example of how the integration can help to detect, rather than just respond to security incidents. Companies are often overwhelmed with information from multiple sources. The JSOC integrates these diverse streams and harnesses it into actionable information. Seeking to build trust, draw down barriers, and share information among these groups in JSOCs can help companies economically and efficiently address multi-vector threats.

References

1. Harris, S. (2013), 'Physical and Environmental Security', in CISSP Exam Guide (6th edn, pp. 427–502), USA: McGraw-Hill.
2. Nakashima, E. (2011), 'Cyber Intruder Sparks Response, Debate', *Washington Post* [Internet], available at https://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html?utm_term=.2b78ddbb7ea0 (accessed 17th January, 2017).
3. Dimensional Research (2016), 'The Growing Security Threat from Insiders: A Survey of IT Professionals', available at http://info.preempt.com/hubfs/InsiderThreatReport.pdf?t=1486167378277 (accessed 23rd January, 2017).
4. Robinson, L. and Henry, T. (2016), 'Building a Risk-Aware IAM Environment with Identity Analytics', Gartner, available at https://www.gartner.com/doc/3249327/building-riskaware-iam-environment-identity (accessed 24th January, 2017).
5. Groysberg, B. (2016), 'Global Board of Directors Survey. Spencer Stuart', available at https://www.spencerstuart.com/~/media/pdf%20files/research%20and%20insight%20pdfs/wcd-board-survey-2016_041416.pdf?la=en (accessed 22nd January, 2017).
6. St. Hilaire, R. (2015), 'Data Security Best Practices Not Good Enough', eSecurity Planet, available at http://www.esecurityplanet.com/network-security/data-security-best-practices-not-good-enough.html (accessed 23rd January, 2017).
7. NERC (2016), 'Grid Security Exercise GridEx III Report', available at http://www.nerc.com/pa/CI/CIPOutreach/GridEX/NERC%20GridEx%20III%20Report.pdf (accessed 25th January, 2017).
8. AVTEST, 'Malware' (2017), available at https://www.av-test.org/en/statistics/malware/ (accessed 25th January, 2017).
9. Lockheed, M. (2014), 'Closing the Gap between Physical, Process Control, and Cybersecurity for the Energy and Utilities Industry', available at http://www.energysec.org/events/summits/energysec-10th-anniversary-security-summit-presentation-archive/ (accessed 24th January, 2017).
10. Hewlett-Packard Development Company (2013), LP. 5G/SOC: SOC Generations.
11. Flammini, F., Setola, R. and Franceschetti, G. (2013), 'Effective Surveillance for Homeland Security: Balancing Technology and Social Issues', CRC Press.