VOLUME FOUR
NUMBER ONE
AUTUMN/FALL 2020

ISSN: 2398-5100

Cyber Security

A Peer-Reviewed Journal

Available online

HENRY
STEWART
PUBLICATIONS

Effectively integrating physical security technology into the operational technology domain

Received (in revised form): 13th March, 2020

Matthew Wharton
President, Strategic Accounts Guidepost Solutions, USA

Matthew Wharton serves as President, Strategic Accounts for the Guidepost Solutions Security and Technology Consulting group and oversees new client acquisition and client retention across its core services, including cyber security, system design and project management, global command and control centres, security assessments and managed services. He is a career security professional with more than 35 years' experience leading security consulting and integration firms. Matthew is currently managing the integration and implementation of physical security within the OT domain as described in this paper for a global Fortune 5 corporation.

Strategic Accounts, Guidepost Solutions, LLC, 1911 Dallas Parkway, Suite 170, Dallas, TX 75287, USA
Tel: +1 469.568.0615; E-mail: mwharton@guidepostsolutions.com

Abstract The operational technology (OT) domain has historically been an area of sensitivity primarily within the industrial (manufacturing, petrochemical, medical) and critical infrastructure (power, water, utility, data, telecommunication) markets. Recent compromises of OT have expanded the exposure to loss from this domain into more core corporate markets, including pharmaceutical, technology, logistics/supply chain, software, banking/finance, retail, warehouse/distribution and commercial office. This paper promotes a holistic countermeasure implementation programme must be put in place and be managed as a core competency within the overall cyber security posture of an organisation in order to effectively mitigate threats to this domain. It advises how physical security controls must be a priority within this posture to effectively control access to the on-site assets that manage OT. The control strategy put forward in this paper introduces two key attributes. The first is to apply physical security controls to protect OT, which may require an expansion of the locations at a site where these controls are deployed. The second is to treat physical security assets as OT so they fall under the same level of network segmentation, threat management, version control and access management as core OT assets.

KEYWORDS: operational technology (OT), convergence, physical security, cyber security, process control, SCADA, robotics, manufacturing security

TODAY'S OT LANDSCAPE

Operational technology (OT) is defined as 'hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise'.[1]

This definition has been applied to the operating environments within enterprises that have relied heavily upon process controls and data acquisition/monitoring platforms within highly-regulated environments.

Recent losses through the compromise of the OT domain[2] have demonstrated that the exposure to OT-related losses have expanded to several markets that previously were not sensitive to this area of cyber security risk. This vector was utilised in a widely known breach that occurred at Target stores wherein the OT layer was compromised via a heating, ventilation and air conditioning (HVAC) control panel in a store that allowed perpetrators to 'tunnel' into the point of sale (POS) network and exfiltrate customer credit card data.[3]

Bringing a company's mitigation strategy into alignment with the current risks within this domain is paramount to protect ongoing operations and their impact on the company's revenue, reputation and shareholder value.

A ROBUST OT DEFENCE POSTURE

Once an organisation understands the true breadth of vulnerability within its control system architecture,[4] the cyber security team can embark upon a programme to stratify these vulnerabilities and the attendant threat vectors to the OT domain.

This programme entails the identification of the key OT assets across the enterprise and assigning a hierarchy of criticality to these assets.

Top-tier assets must be segregated by several layers of protection from lower-tier assets to reduce the exposure to threat vectors from the compromise of the higher quantity of instances of IT assets across the lower tiers.

This robust assignment of tiers and hierarchy should follow industry best practices and allow for effective segmentation across the network infrastructure and applications.[5]

This understanding and categorisation will allow for a converged and integrated physical and logical security architecture[6] that will establish the protection protocols, policies and devices that will enforce data security, access and segregation between assets subject to segmentation.

This 'pyramid' approach will result in a small number of key assets at the top of the network hierarchy and segmentation, with increasing numbers of less-critical assets populating the structure and base of the pyramid (see Figure 1).

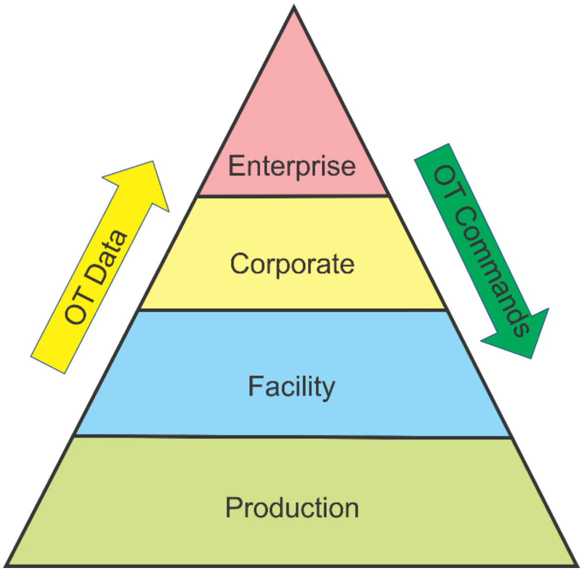

Figure 1: Network asset hierarchy
Source: Author

Enterprise assets are the key applications and data sets that govern the organisation, inclusive of cyber and physical security monitoring and command and control assets. Corporate assets include all financial, human resources (HR), legal and compliance platforms and data that intersect between the enterprise layer and the lower tiers of the hierarchy. Facility assets are the systems and infrastructure that allow both administrative and production facilities to operate. Production assets are the systems and controls that govern the generation of the company's product and manage the corporate supply chain. OT platform and device data flow upward through the tiers from the facility and production levels, and OT command and control data flows downward from the higher tiers of the organisation.

This hierarchy of assets and their inherent integration resonate with the current designation of the evolution of manufacturing and product delivery to 'Industry 4.0'.[7] This term encompasses the next level of interconnectivity of computer and data resources within the product and revenue creation functions of an organisation. This increased integration and interconnectivity brings with it the inherent need to apply a greater level of security oversight and control over the interconnected systems and devices.

Assets designated as OT which require this oversight and control may reside in any (or all) of these tiers, as indicated in Table 1:

Table 1: Propagation of OT assets

Tier	Potential OT assets
Enterprise	IT oversight of OT platform command and control centres and infrastructure
Corporate	IT oversight of OT platform reporting applications and historical/trending data sets
Facility	Building management systems (BMS), physical access control systems, networked video surveillance (NVS) systems
Production	Manufacturing control systems, robotics, SCADA, material handling/scanning applications, supply chain monitoring and management platforms

A comprehensive workflow should be established to identify each platform and device that is designated as OT across the enterprise. Once OT designation has occurred, true OT network segmentation can be accomplished.

OT assets should be, at a minimum, logically segregated using secure virtual local area network (VLAN) and firewall connections to separate OT assets from the company's core administrative network. Ultimately, segregation at a hardware level (dedicated switches in the field handling only OT assets) is preferred but can be challenging especially when being deployed across an infrastructure that was installed prior to the identification of the sensitivity of OT assets. If retroactively applying a physical segregation should be deemed unfeasible due to budgetary or service level constraints, a 'hybrid' approach should be taken wherein new instances of OT should be physically segregated while legacy systems can remain logically segregated across the network.

The logical (or physical) segregation should be deployed to simultaneously to partition OT assets *from non-OT* networks and devices and *from other OT platforms*. This platform-specific segregation will allow for the isolation of a specific OT platform from other enterprise assets should a credible threat be discovered that targets this hardware or software, or should an actual threat agent be detected within the specific OT segment.

With this segmentation and segregation in place, a 'drawbridge' strategy can be developed to allow for the isolation of a specific lower tier of the overall network asset pyramid from the more critical tiers above a compromised domain.

A holistic monitoring and mitigation programme should be in place utilising security information and event management (SIEM)[8] and other platforms to effectively enforce targeted cyber intrusion and detection and mitigation strategies.[9]

This 'drawbridging' will keep a facility or production platform compromise from propagating across the overall network which can create the catastrophic level of business disruption and financial impact referenced at the beginning of this article.

PHYSICAL SECURITY TO ENFORCE OT NETWORK SEGMENTATION

The logical segmentation of the OT network will minimise the exposure to the introduction and propagation of threat agents within the OT domain and the cross-network compromise of core corporate IT assets from these agents.

To further bolster these logical security measures under the governance of the cyber security team, the company's physical security team must be engaged to limit and normalise the physical access to the on-site OT assets that reside across the enterprise.

This programme will introduce the

concept of using physical security devices and platforms to *protect OT*.

The implementation of physical security devices to protect OT must be accomplished in a holistic fashion between key stakeholders within the company's physical security, IT security and OT operations/security departments to empower an integrated and interconnected approach top addressing zero one tech (ZOT) security vulnerabilities.

The core concept of physical security control is to standardise the application of physical security countermeasures in a layered, defence-in-depth approach that segregates the company's most critical assets behind several concentric rings of physical security countermeasures, as represented in Figure 2.

The facility perimeter is defined as the area that is accessible to the public before the first security barrier is reached. This area includes driveways, walkways, loading docks, visitor parking and any other grounds accessible to the general public. Facility perimeter area security should be developed and deployed utilising crime prevention through environment design (CPTED)[10] best practices, physical security technology systems and non-technology elements including fencing, landscape design, lighting and bollards/vehicle control solutions.

The public space at each facility is defined as those areas within the security perimeter where the general public (visitors, contractors, temporary employees, curious passers-by, etc.) are allowed to enter and be identified by the facility's personnel. Public space areas include the main lobby and the loading dock area.

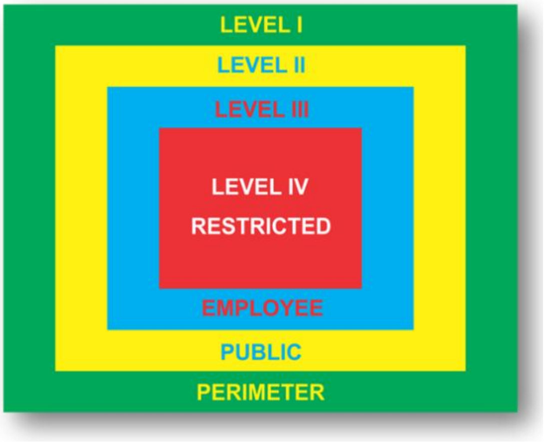

Figure 2: Physical security protection levels
Source: Author

The public space may be unlocked during normal business hours if a there is an appropriate number of company personnel posted in the area to control the flow of visitors, contractors, temporary employees and other personnel entering the facility.

A security portal must be implemented within the public space for the proper identification and badging of visitors and for notification of facility employees who may need to come to the public space to escort a visitor. Adequate space should be provided for a waiting area that is under scrutiny by company personnel for visitors to await their escorts.

The next security level within the facility is the employee space. This space is defined as the area where facility employees, contractors and authorised temporary employees are allowed access to perform their routine work assignments.

All visitors while within the employee space should be escorted. Visitor and employee badges should be worn in plain view to facilitate the challenging of any personnel seen within the employee space without a proper security credential.

The separation between the public space and the employee space should contain an electronic access control portal to ensure that only authorised and approved personnel enter the space and an intruder or a terminated employee or a contractor with an expired or deleted access credential may not enter the space. This access control portal should be under constant viewing and recording from a networked video surveillance (NVS) system.

Restricted space is the highest level of security within the facility and addresses those areas that contain facility assets and information that should not be accessed by the general employee population. Examples of these sensitive areas are network equipment rooms, control (OT) equipment rooms, network traffic areas, HR/legal/finance areas and computer rooms.

Access to restricted space areas should be through portals controlled by electronic card access control readers. The security system should be programmed with enough access levels to only allow those personnel with a specific need to be in each restricted space area.

Proper application of physical security countermeasures within the restricted space to effectively *protect OT* may require an on-site assessment of how current physical security countermeasures are implemented and their current coverage of specific OT assets.

The traditional application of physical access controls and NVS monitoring at facilities encompassed core company assets including IT infrastructure both in computer rooms and in intermediate distribution frame (IDF)/building distribution frame (BDF) rooms.

The deployed OT assets at a facility may be collocated within these rooms, but there may be a broad spectrum of process control or manufacturing control assets (programmable logic controllers [PLCs], distributed processors, production line automation controllers, etc.) that are deployed within cages or other areas across the production floor.

Gathering and documenting these locations will allow the company to determine additional access control methodologies to limit the personnel who can physically put hands on these assets, preventing potential system compromise or the introduction of third-party eavesdropping equipment to potentially implement a man-in-the-middle (MITM) attack.[11]

The implementation at the facility level of physical security technology should be governed by a physical security standard developed by the company's security department and approved by all key stakeholders (real estate, facilities, IT, etc.) to ensure that these devices and mitigation measures are applied in a consistent fashion across all facility types.

Monitoring and incident management for physical security technology should be further governed by a documented and auditable concept of operations (CONOPS)[12] that guarantees adherence to best practices in the consumption of alert data from the field and the establishment of corrective actions to be taken by the security department in responding to and resolving site incidents.

TRANSITIONING PHYSICAL SECURITY ASSETS TO THE OT DOMAIN

Many organisations categorise physical access control, security and NVS systems and devices as facility-based assets. Moving these assets into the OT domain significantly increases their risk-management value to the enterprise and introduces several layers of management and oversight that are not typically required from a facility-only asset.

This reclassification, standardisation and implementation of a more holistic and robust physical security protection layer will enhance and enforce the network segregation strategies of the overall OT security protection initiative.

Concurrent with this implementation should be the reclassification of physical security devices and platforms from segregated assets under the management of the corporate security department to core OT assets under the governance of the overall OT programme management.

This evolution from physical security assets *protecting OT* to physical security assets being treated *as OT* has many far-reaching implications and workflows which are expanded upon in detail, including:

- Project management;
- Asset management;

- Identity access management (IAM);
- Service ticket management;
- Patch management;
- Disaster recovery (DR)/business community planning (BCP) management;
- Joint special operations command (JSOC) monitoring.

Project management

The project management workflow needs to support the concurrent implementation management of applying physical security technology with company standards and the assimilation of these devices into the OT landscape.

This is accomplished via extensive design, engineering and documentation of the physical security countermeasures that deliver device-by-device graphical representations of what is being installed at each facility, combined with programming documentation for how these devices will be integrated to support the overall security CONOPS.

The project management function must also focus on not only standard construction administration (making sure that all devices that were procured are installed per specifications) but also on a robust and comprehensive programme for the documentation of system commissioning.

Each protected portal at a facility containing OT assets must have all of its monitorable functions confirmed (in the case of physical access control, this would include states such as access granted, access denied, door forced open, door held open, reader data loss, reader data restore, tamper active, tamper clear, etc.).

This baseline confirmation would be augmented by the confirmation of all downstream integration functions (NVS camera call-up, increased recording resolution, operator commands, map/graphic call-up) along with documentation of all functions on a portal-by-portal basis.

Asset management

The detailed project management documentation can now be utilised to support the asset management tasks required to catalogue and document the installed inventory of physical security assets across the enterprise.

Table 2 shows the minimal data set required for this asset management programme includes, by physical security device connected to the network.

Capturing this documentation of the installed physical security asset inventory will allow for the core business functions of life cycle management and service trending along with the enhanced capability to effectively monitor and mitigate threats to these devices and their underlying network connections.

Vulnerabilities to Internet Protocol (IP)-based security devices are common, and the company needs to be in a position to rapidly ascertain whether it has any instances in its network of compromised devices, where these devices reside physically, where they are connected logically and what the potential remediation effort is to correct a compromise.

This corrective measure could be as simple as an updated firmware ‘push’ to the affected devices or as complex as disabling the affected devices connection to the network until their compromise can be manually remediated.

Assimilating these data points into an asset management programme will automate the discovery and remediation efforts required to manage potential compromises to resolve issues in hours instead of the days that could be required in a manual process.

Table 2: Asset management data fields

• Date placed in service	• Device manufacturer/ model #
• Serial number	• Physical location
• IP address	• Firmware version
• Environmental conditions	• Anticipated life cycle

Identity access management (IAM)

Converged and integrated IAM must be applied across both the physical and logical access control domains to enforce the company's OT protection posture.

In a converged environment, employee access rights are governed by a converged database that consumes and manages data from the IT/cyber security organisation, HR, the security organisation and contract (third-party resources) management.

A benefit of this convergence is to allow for more convenient onboarding of personnel (any stakeholder department can request and pre-populate access requests). A more compelling business support element is the ability of any single department to revoke access rights and have this revocation cross-populate to the other affected domains. At many companies this is a manual and time-consuming process with disparate data sets and access privileges dispersed across the enterprise.

In an environment of robust OT protection, a person who has been identified as a risk must have all privileges revoked in a timely fashion. This is especially pertinent within the OT context, since many of the individuals who have logical access privileges to the platforms and systems identified also have physical access rights to programme and maintain these assets.

Besides immediate revocation of privileges, converged IAM environments[13] can also allow for dual authentication of access requests for critical OT platforms. This convergence aligns a logical access request (through active directory [AD] or other logical identity management portal) with a physical location confirmation that the requester is actually in the facility/area where the equipment they are accessing resides.

Service ticket management

The traditional model for service ticket management for a facility-based asset is to dispatch a service vendor to 'roll a truck' and head to the site to troubleshoot and correct a reported system issue. This model can introduce response times for service from 4 to 36 hours from when the service call is placed and repair times starting at another 4 to 36 hours from when a technician arrives on site.

When these assets move to mission-critical risk management devices, this service model introduces inadequate response and remediation times and increased long-term operational costs.

With the transition of security devices to IP-connected network appliances, the service management of these appliances should follow the established workflow of core IT service support.

A triage model should be put in place to ascertain whether an apparent device failure is in fact the endpoint device, or if it is an interruption of services (network, power, processing, etc.) between the endpoint device and the monitoring workstation.

Typical security devices have a five to ten-year useable life cycle, so in most instances of service ticket creation the root problem is not the endpoint device.

Properly trained and experienced technical resources can triage and remediate these service disruptions within the physical security layer and bring devices back online in minutes instead of hours or days. Only when a true endpoint device failure is confirmed would there be a requirement to 'roll the truck' and have a service vendor repair or replace the device, with its inherent costs and time delays.

Typical security system installation and service contractors do not have the technical acuity to perform this level of triage and network-centric troubleshooting services. There are independent managed services providers within the physical security market that can provide this level of support.

The key to success in provisioning and maintaining this service ticket management environment is to establish a single, enterprise-wide physical security technology 'help desk' wherein all service issues are reported directly to the triage team, service vendors are only dispatched when warranted, and all key performance indicators (KPIs) for mean time to respond and mean time to repair along with service and maintenance costs are captured within this entity.

In our experience providing third-party managed services for global organisations and managing thousands of service tickets annually, we have found that over 75 per cent of service requests can be resolved via triage with mean times to respond at less than 30 minutes and mean time to repair at under one hour with no exposure to outside service vendor expenses.

The asset management database should also be appended to provide these additional fields to assist in the trending and mitigation of repeat trouble or service problems from a specific facility or device (see Table 3).

Table 3: Additional asset management fields

• Last service date	• Service/trouble frequency #
• Last false alert date	• False alert frequency

A normalised process should be in place for the service ticket workflow (see Figure 3) and verification of the resumption of services with the requester in the field. This drives end-to-end documentation and auditability of the process and ensures user group involvement and satisfaction with the service levels provided.

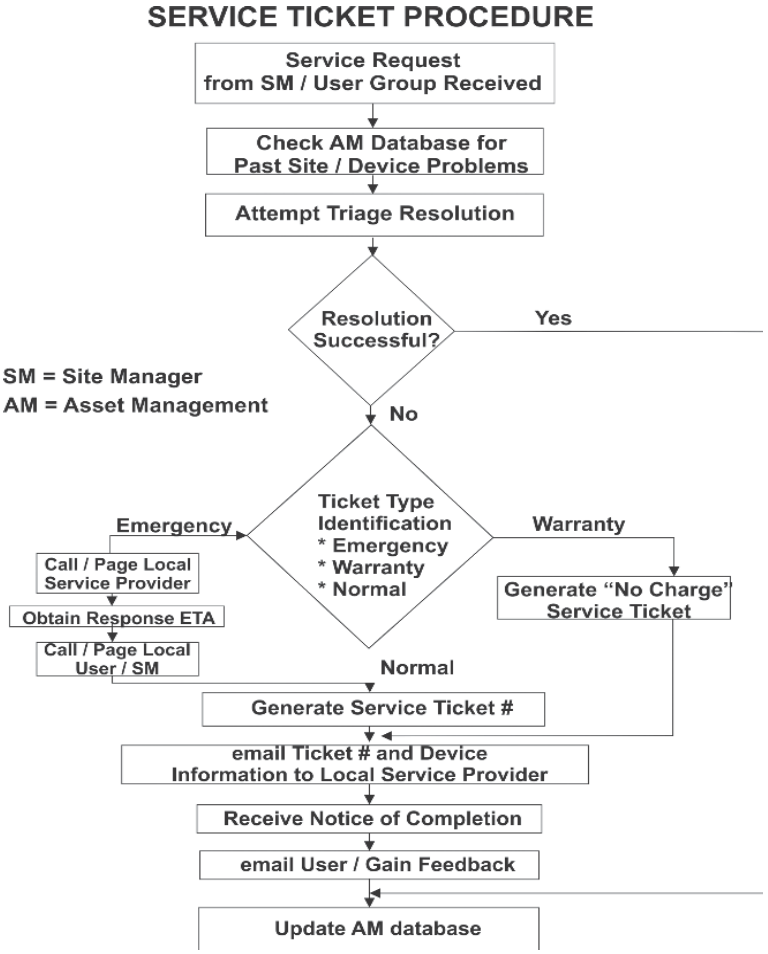
SERVICE TICKET PROCEDURE
Service Request from SM / User Group Received
Check AM Database for Past Site / Device Problems
Attempt Triage Resolution
Resolution Successful?
Yes
SM = Site Manager
AM = Asset Management
No
Ticket Type Identification
* Emergency
* Warranty
* Normal
Emergency
Warranty
Call / Page Local Service Provider
Obtain Response ETA
Call / Page Local User / SM
Generate "No Charge" Service Ticket
Normal
Generate Service Ticket #
email Ticket # and Device Information to Local Service Provider
Receive Notice of Completion
email User / Gain Feedback
Update AM database

Figure 3: Service ticket procedure
Source: Author

Patch management

Maintaining security and version control integrity across the physical security assets that are categorised as OT is paramount for their continued defence of company assets and their intrinsic defence posture against cyber security compromise.

Patch management of physical security technology as OT involves three distinct workflows with their own unique domain owners and cadence: operating system (OS) updates, application-specific updates, and threat-specific remediation patches.

OS updates (particularly from Microsoft) are on a bi-weekly cadence. Typical OS patch management is governed within an organisation from the IT department's utilisation of a version control agent that propagates the updates to all machines within the company's domains, which would include servers, workstations and network video recorders (NVRs) within the physical security space.

Some manufacturers of these systems have an OS update verification process to confirm there are no operational issues with these updates to their applications in the field. This verification process normally trails the OS update by 2–3 days. Exceptions are reported to clients so they can apply the approved patches and delay implementation of an OS patch that may present an issue.

While these exceptions are not a weekly (or even monthly) occurrence, they should be taken into account in the cadence of OS patch propagation to the physical security platform machines to allow for exceptions and to avoid causing any interruptions of service.

Application-specific updates within the physical security platform usually include an annual full version upgrade as part of an ongoing software support agreement (SSA) with the manufacturer. Inter-version updates to address software issues are distributed as required approximately on a quarterly cadence. This workflow also includes firmware updates for IP-connected devices such as control panels and NVS endpoint cameras.

Table 4: Patch categories/cadence/owners

Patch category	Cadence/owner
OS	Weekly. IT OS management agent in coordination with physical security
Application/firmware	Annual + ≈ quarterly. Physical security
Threat-specific	As required. IT and protection software provider in coordination with physical security

Application-specific updates would not be governed by the IT agent, since these programming initiatives often require stopping the services of the affected devices and should be scheduled and overseen by the security organisation.

Threat-specific remediation patches are most often distributed from the company's cyber security protection software provider in response to a particular virus or malware vulnerability.

These patches are applied by the IT security organisation and should be coordinated with the physical security platform stakeholders to ensure they do not interrupt downstream system operations.

The physical security technology 'help desk' can act as a key point of coordination for all of these patch initiatives to ensure proper version control, communication with the IT organisation and maintenance of maximum system uptime in the field.

DR/BCP management

A compromise within the OT domain will have far-reaching impact across any enterprise, inclusive of triggering disaster recovery (DR) and business continuity planning (BCP) teams and workflows.

The IT organisation, the cyber security team and the physical security team need to organise and document their response protocols to support DR and BCP efforts in the event of a compromise and the downstream recovery efforts to allow for resumption of normal business activities.

This proactive posture should be bolstered by work sessions and table-top exercises to assign leadership and support roles in advance of an incident. This will ensure the most effective management and coordination of efforts in the event of an actual compromise.

The scrutiny and drive from executive leadership in one of these incidents will be intense, and all team members should be prepared for their assigned tasks and have drilled these tasks in a simulated environment to be able to adequately handle this pressure in a live response scenario

JSOC monitoring

A successful OT protection programme exhibits convergence between IT infrastructure, cyber security and physical security on several levels, as previously detailed. This convergence should not break down at the command and control level of the organisation.

Merging and integrating the monitoring of cyber security and physical security into a collaborative JSOC environment will allow for the rapid response to threats or compromise and the immediate application of remediation efforts to address issues in the field.

Analysts from both disciplines should be collocated and cross-trained to maintain deterrence countermeasures, detect threats and risks, and to respond effectively in a cross-disciplinary and collaborative fashion.

CONCLUSION

OT has emerged as a mission-critical core business asset that can have grave ramifications for the company's revenue, reputation and shareholder value if compromised.

A converged and cross-functional approach must be taken to address the protection of the OT domain, with physical security technology assets playing a key role in this protection landscape.

Applying physical security in a standardised and documented fashion to protect potential vulnerabilities is a prudent business decision and should be a key component in an overall OT and IT security management programme.

As these countermeasures are applied, they represent an attendant investment in an additional platform that will be categorised as OT and all assets under this domain should be applied, monitored and maintained under the same strict disciplines that apply to other mission-critical appliances and applications.

References

1. NIST, 'Operational Technology', Computer Security Resource Center Glossary, available at https://csrc.nist.gov/glossary/term/operational_technology (accessed 21st May, 2020).
2. Nash, K. S. (June 2017), 'One Year After NotPetya Cyberattack, Firms Wrestle with Recovery Costs', *Wall Street Journal*, available at https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906 (accessed 21st May, 2020).
3. Radichel, T. (August 2014), 'Case Study: Critical Controls that Could Have Prevented Target Breach', SANS Institute Information Security Reading Room, available at https://www.sans.org/ reading-room/whitepapers/casestudies/case-study- critical-controls-prevented-target-breach-35412 (accessed 21st May, 2020).
4. Cybersecurity & Infrastructure Security Agency, 'Understanding Control System Vulnerabilities', available at https://www.us-cert.gov/ics/content/overview-cyber-vulnerabilities#under (accessed 21st May, 2020).
5. Cisco, 'A Framework to Protect Data Through Segmentation', available at https://tools.cisco.com/security/center/resources/framework_segmentation (accessed 21st May, 2020).
6. NIST, 'Security Architecture', Computer Security Resource Center Glossary, available at https://csrc.nist.gov/glossary/term/security_architecture (accessed 21st May, 2020).
7. Marr, B. (September 2018), 'What is Industry 4.0?', *Forbes*, available at https://www.forbes.com/sites/bernardmarr/2018/09/02/what-is-industry-4-0-heres-a-super-easy-explanation-for-anyone/#4e5db2f59788 (accessed 21st May, 2020).
8. Gartner, 'Security Information and Event Management (SIEM)', Garner Glossary, available at https://www.gartner.com/en/information-technology/glossary/

security-information-and-event-management-siem (accessed 21st May, 2020).

9. Cybersecurity & Infrastructure Security Agency (February 2013), 'Targeted Cyber Intrusion Detection and Mitigation Strategies', available at https://www.us-cert.gov/ics/tips/ICS-TIP-12-146-01B (accessed 21st May, 2020).
10. ICA, 'Crime Prevention Through Environmental Design (CPTED) definition', available at cpted.net (accessed 21st May, 2020).
11. Cybersecurity & Infrastructure Security Agency (April 2015), 'Alert (TA15-120A) – Securing End-to-End Communications', available at https://www.us-cert.gov/ncas/alerts/TA15-120A (accessed 21st May, 2020).
12. NIST, 'Security concept of operations (Security CONOP)', Computer Security Resource Center, available at https://csrc.nist.gov/glossary/term/security_concept_of_operations (accessed 21st May, 2020).
13. HID Global, 'The Convergence of Physical and Logical Access: What it Really Means for an Organization's Security', available at https://www.hidglobal.com/doclib/files/resource_files/the_convergence_of_physical_and_logical_access_-_whitepaper_final.pdf (accessed 21st May, 2020).