UNISYS

Enhancing National Cybersecurity: The Current and Future States of Cybersecurity in the Digital Economy

Prepared by

Tom Patterson
Ed Liebig
Rodd Sapp
Bill Searcy
Dhimant Desai
Chris Blask
John Bone
Scott Spiker

Unisys Corporation
801 Lakeview Drive, Suite 100
Blue Bell, Pennsylvania 19422

This document was prepared by Unisys for the National Commission on Enhancing National Cybersecurity and the National Institute of Standards and Technology. Tom Patterson, Chief Trust Officer and Vice President of Global Security at Unisys, led the project.

Table of Contents

Executive Summary

Unisys is proud to support President Obama's Commission on Enhancing National Cybersecurity, as directed by Executive Order 13718. As a critical technology partner to both Government and industry, one that has been at the forefront of every major technological change for over a century, Unisys is pleased to offer the Commission as well as the National Institute of Standards and Technology (NIST) unique perspectives and recommendations for securing the future of the digital economy.

Unisys understands that, in today's digital economy, interdependence is more critical than ever, and that the failure of one may well effect the future of many. As a company that delivers leading physical security and cybersecurity solutions to organizations around the globe, Unisys sees first-hand the growing sophistication and persistence of both foreign and domestic threats. As a provider of global solutions in such industries as transportation, finance, government, healthcare, energy, and more, the company takes an integrative approach in addressing threats. Unisys views trust and security as the most critical building blocks for the future, and is committed to using them to help secure a future that will benefit everyone.

In the pages that follow, Unisys provides security, privacy, and trust recommendations in the areas of Critical Infrastructure, Research and Development, Federal Governance, Identity and Access Management, and the Internet of Things.

Among key observations is the recognition that enterprises are no longer restricted within a controlled perimeter, requiring a fresh security strategy for integrated ecosystems. Highlights include the trending use of micro-segmentation technologies to provide more agile and efficient methods of segmentation inside of a modern network, while still enabling the secure use of third-party clouds and integrated supply chains so vital to today's enterprises.

Of note in the Identity and Access Management space, are the following:

- The value of integrating physical security with cybersecurity.
- The growing near-term trend toward user-centric identity to drive security models.

- The use of physical and behavioral biometrics.
- A long-term trend toward trust as a service.
- Distributed trust models with blockchains, useful in many third-party trust equations and vital for a secure Internet of Things (IoT) scale.

Additional areas of recommendation include the elimination of passwords, the rise of big data analytics, the advancement of artificial intelligence, and the establishment of robust situational awareness – including consequences, technologies, and threats.

On the Research and Development front, Unisys targets the development of new technologies with which adversaries are unfamiliar. These include:

- Deploying encryption in motion across all platforms
- Using agile methodologies with DevOps
- Building in security by design

In the area of public awareness and education, Unisys' use of consequence-based assessments and Wargaming is highlighted as a current trend that is proving to be effective.

Overall, while intimately familiar with the current and future states of the cyber threat environment, Unisys remains optimistic that, with the proper application of new security technology and approaches, and strong public-private partnerships, we can use security to enable a future that is both robust and resilient.

Circumscribing Liability and Fortuity: Assessing Risk in ICS Cybersecurity

Background

Wake up calls have been heard: Stuxnet successfully crippled its target. Aramco suffered significant impacts from the Shamoon (Disttrack) malware attack and, it has been speculated, the same Flame Worm variant also struck RasGas. Times have indeed changed, and how we approach Cybersecurity in ICS environments has to change in order to keep pace with evolving threats.

Sixteen years ago, a disgruntled sewer system operator in Maroochy Shire, Australia filled his car with laptops and radio equipment he allegedly pilfered from his employer, and then went on a joy ride of disruption. The incident served as one of the first indications that the present was going to look a good bit different than the past.

The worker was responsible for opening valves, re-routing water, and sending raw sewage into local waterways and creeks. Besides the health hazard and stench the incident produced across the region, the rogue actor brought attention to the damage that could be wrought with proper equipment, know-how, and the Internet-accessibility of ICS equipment and operations.

A cyberattack that hit Brazil in 2007 caused more than three million people to be plunged into total darkness. This knocked the world's largest iron ore producer offline, and cost one company alone a sum of $7 million. A demonstration at Idaho National Laboratories proved that a cyber-based attack could have the capacity to physically destroy capital equipment, in this case a large diesel generator. This fact strikes fear into the hearts and minds of ICS Systems owners and operators. Generators, centrifuges (such as those destroyed by Stuxnet), and similar pieces of "big ticket" equipment are not only costly but, in many cases, not readily available for replacement after an attack.

Overview

ICS Systems are a compilation of traditional IT operating systems and components (like processor chips), with proprietary system components and operating systems, as well as common and proprietary network protocols. Most equipment in the Operational Technology (OT) environment is designed for a 10- to 20-year lifespan, so that much of what is being used today was designed and implemented well before ubiquitous security controls were built into these components. This complicates any hope for homogenization of OT equipment or security strategies across the corporate OT enterprise, or even across a single plant. It presents a need for exacting where to begin and why. It calls for a risk assessment process.

A New Paradigm for Risk Assessments

The operational paradigm has forever changed. No longer are ICS OT environments completely isolated from IT networks. The desire to gain business intelligence from the operational environment has opened up conventional "air-gapped" technologies, thereby connecting OT to IT. This connection, as well as the business drivers for remote administration, has opened up opportunities for exploitation. Looking closely at the "wake up calls" – the significant cyber events described earlier – it is clear that they represent a specific call to action: the risk assessment paradigm must change.

The risk assessments conventionally used by the insurance, legal, and IT communities constitute a four-step process. First, a list of previously encountered business threats should be compiled. Then, other threats (if known or foreseeable) can be added to the list, to reflect current or future concerns. Once this is done, threats are assigned a probability based on their likelihood of occurrence. Next, the cost to the bottom line in lost income is estimated along with the added expense of containing each individual threat. Finally, this estimate is multiplied by the probability of occurrence to determine the company's annual loss exposure (see Figure 1).

Figure 1: Calculating Annual Loss Exposure[1]

hreats Facing the Firm	**Annual Probability**	**Estimated Financial Loss**	**Annual Loss Exposure (ALE)**
Severe Weather	12%	$80,000	$9,600
Earthquake	0.50%	$450,000	$2,250
Prolonged Loss of Power	5%	$210,000	$10,500
Pandemic	1%	$575,000	$5,750
Fire	3%	$280,000	$8,400
Loss of IT Services	10%	$375,000	$37,500
Total Annual Loss Exposure			**$74,000**

The arguable challenge with traditional risk assessments is the representation of "probability." With attacks on ICS rising in just the past 5 years, any metrics used to

[1] Donald Byrne, "Consequence-Based Analysis: An Emerging Risk Assessment Paradigm," April 2011, available from LawPracticeTODAY. Accessed on September 7, 2016 at https://www.americanbar.org/publications/law_practice_today_home/law_practice_today_archive/april11/consequence-based_analysis.html

justify probability are suspect. The threat vectors are also vague and in motion. Therefore, predicting probability is also skewed from that perspective.

A Consequence-Based Approach

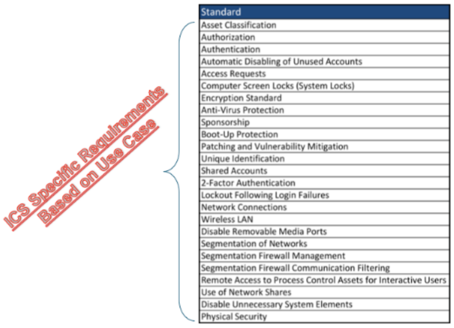
The aforementioned are the reasons why the ICS industry has gravitated toward a consequence-based risk assessment process. Unisys employs such a methodology and process to better present a business case for action and "heat-map" the OT environment for levels of risk and cybersecurity rigor. What follows is a simplified depiction of Unisys' more complex framework.

The consequence-based approach relies less on asking "What could happen?" and "What if something happens?" and moves instead to exact the following: "When something happens, how bad will it be?" The focus is on mitigating controls to minimize impact.

> UNISYS believes that a consequence-based risk assessment is the essential approach for the current threat landscape. Estimating probability is futile.
>
> Edward Liebig VP, Security Services

> A consequence-based approach provides a defensible and useful identification of critical infrastructure entities.
>
> Cyber-Dependent Infrastructure Identification Working Group (CDIIWG)

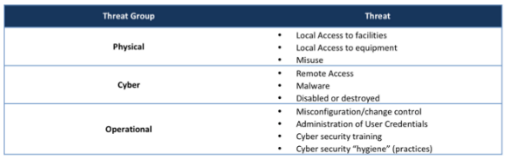
For the ICS environment, this means that standards become the mitigation for minimizing the consequence of compromise. Standards must be created specifically for the OT environment, since traditional IT standards do not function operationally in OT. This means that traditional IT standards must be assessed in order to determine their true "spirit." Standards for the OT


ICS Specific Requirements
Based on Use Case

Standard
Asset Classification
Authorization
Authentication
Automatic Disabling of Unused Accounts
Access Requests
Computer Screen Locks (System Locks)
Encryption Standard
Anti-Virus Protection
Sponsorship
Boot-Up Protection
Patching and Vulnerability Mitigation
Unique Identification
Shared Accounts
2-Factor Authentication
Lockout Following Login Failures
Network Connections
Wireless LAN
Disable Removable Media Ports
Segmentation of Networks
Segmentation Firewall Management
Segmentation Firewall Communication Filtering
Remote Access to Process Control Assets for Interactive Users
Use of Network Shares
Disable Unnecessary System Elements
Physical Security

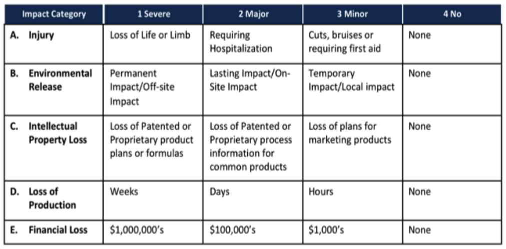
environment are then devised accordingly (based on use case).

The threat vectors are less important, since only the results of a compromise are considered. Threats are boiled down to their most rudimentary vector. Consequences resulting from a compromise in these categories are then recorded for each component of the ICS infrastructure.

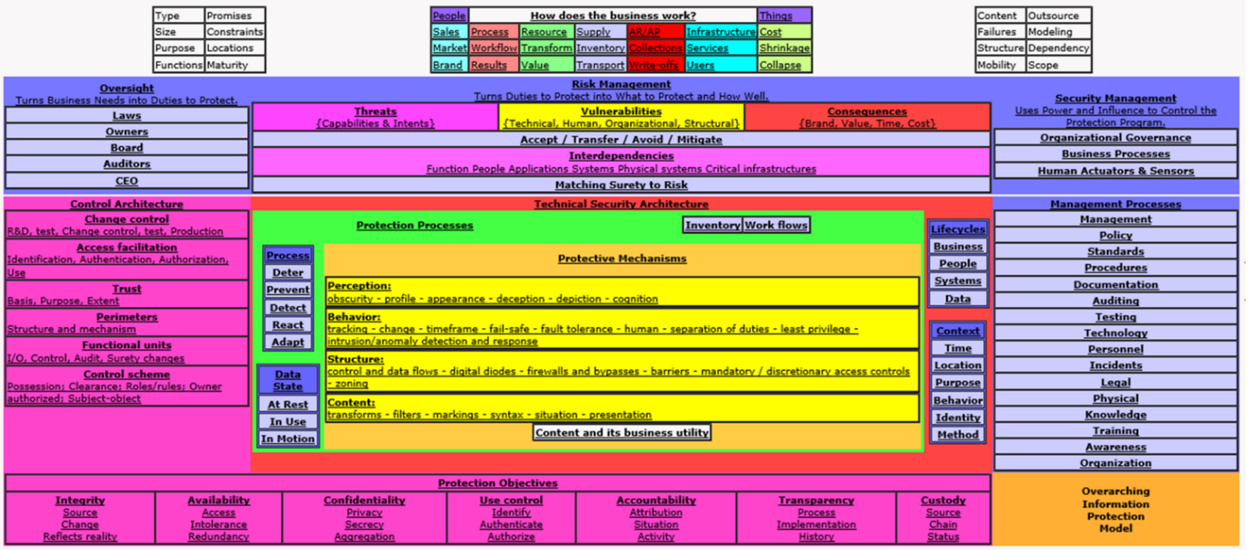


Threat Group	Threat
Physical	• Local Access to facilities • Local Access to equipment • Misuse
Cyber	• Remote Access • Malware • Disabled or destroyed
Operational	• Misconfiguration/change control • Administration of User Credentials • Cyber security training • Cyber security "hygiene" (practices)

The next key challenge is to establish the tolerance for risk in the organization – determining what is important to measure and the degree of impact severity (i.e., life, health, and safety; environmental protection; intellectual property; production loss or financial impact). Setting levels for tolerance allows the assessor to articulate the impact if a device or component of the OT environment is compromised.



Impact Category	1 Severe	2 Major	3 Minor	4 No
A. **Injury**	Loss of Life or Limb	Requiring Hospitalization	Cuts, bruises or requiring first aid	None
B. **Environmental Release**	Permanent Impact/Off-site Impact	Lasting Impact/On-Site Impact	Temporary Impact/Local impact	None
C. **Intellectual Property Loss**	Loss of Patented or Proprietary product plans or formulas	Loss of Patented or Proprietary process information for common products	Loss of plans for marketing products	None
D. **Loss of Production**	Weeks	Days	Hours	None
E. **Financial Loss**	$1,000,000's	$100,000's	$1,000's	None



By reducing dependency on probability estimating, the risk assessment process becomes more relevant as well as more timely. By focusing on a limited number of risk categories and applying these across all key components of the OT infrastructure, assessors can ascertain what initiatives will need to be undertaken within a plant. This ensures that security standards are in place, regardless of the threat vector or method. Moreover, this information easily drives project estimates as well as budget requirements. Capital spending can be directed at specific areas, and the decision to spend money can be justified in part by knowing that a business decision was not based on one or two single threats.

Summary

The recommended improvements will help to protect the OT environment against foreseeable and unforeseeable threats. Experience shows that these changes often lead to expense savings, improved productivity, enhanced morale, and increased revenues. Focusing on the segments of the operation that would be impacted during a disruption is emerging as a successful management practice. Consequence-based risk assessments provide all the benefits of conventional methods while eliminating the uncertainty associated with other approaches.

Cybersecurity Research and Development

Overview

In today's continuously evolving threat landscape, cybercriminals possess as profound an understanding of existing network security as do the best of corporate IT professionals. This presents unique challenges for cybersecurity product vendors. Primarily, these vendors are required to be continuously innovating in order to stay a step ahead of cybercriminals.

To this end, cybersecurity product vendors must:

1. Keep research and development focused on the formulation of new technologies that are both unfamiliar to cybercriminals and which can prevent, or at least limit, their activities.
2. Make rapid iterations to products in order to keep addressing the most current (as well as future) threat vectors.
3. Design products that secure a broad range of environments—from small datacenters to hyper-scale multi-cloud infrastructures.

A Promising Technology

A leader in cybersecurity research and development, Unisys has received numerous innovation and security product-of-the-year awards for its Unisys Stealth® micro-segmentation technology. Stealth takes a disruptive posture to existing perimeter security topologies – which have been built with firewalls, routers, switches, and layers of security software. Stealth goes beyond merely securing the perimeter to conceal (or cloak) critical corporate assets and keep these from becoming the targets of cybercriminals.

Unisys' development resources are recognized throughout the country, as are its subject matter experts, whose deep cybersecurity expertise and renowned best practices make it possible for clients to face the growing and increasingly sophisticated cyber threats they continue to encounter.

Stages of the Process

Unisys' cybersecurity research and development process begins with its Innovation Practice—a Lean StartUp influenced by a methodology that favors experimentation in lieu of elaborate planning, client feedback over intuition, and iterative design over large, conventional, up-front design.

In this first phase, ideas are generated based on inputs from employees, detailed primary research conducted with customers, partners and internal sales teams, as well as input from leading technology analysts and secondary research.

Viable ideas are then refined via further primary research and exploration to create an initial business model canvas and, if warranted, a Proof of Concept (POC) proposal. (POCs are designed to validate hypotheses, and business and technical assumptions are derived from the idea maturation phase.)

The final research and development stage involves producing a Minimum Viable Product (MVP) with the goal to get to market. A dedicated team then proves or disproves market hypotheses through early adopters, and adjusts accordingly. Throughout the process, metrics are collected to evaluate progress against internal benchmarks. The use of agile experimentation and prototyping, along with rapid decision-making on whether to persevere, pivot, or stop further work, helps bring the innovation to market faster than traditional stage-gate product development methodology.

The Unisys cybersecurity development process follows the Agile methodology with DevOps techniques used for accelerating the development and testing cycles.

While Unisys' research and development process is similar across all application development, refinements are made for cybersecurity. These include:

1. The rapid establishment and dismantling of secure lab environments in the public cloud for testing at hyper-scale.
2. Penetration testing by an internal audit team at multiple stages so that vulnerabilities are detected and addressed early in the lifecycle.
3. Early adoption by an internal IT team for their own dev/test and production environments – on-premise as well as in the cloud.

Trends and Future Challenges

Today's enterprise network is no longer restricted to within-the-perimeter. Instead, it stretches across multiple clouds all the way to end-user devices – such as remote PCs, mobile devices, and IoT devices – introducing multiple new threat vectors.

With software IP becoming the key differentiator for enterprises, Unisys foresees an increased threat of cyber-espionage in the coming decades. The risk is exponentially higher for cybersecurity vendors, whose code base offers a lucrative target for hackers.

Recommended Actions

To address such threats, Unisys strongly recommends logical access control to source code and binary repositories on a strict "need-to-know" basis – powered by a single authentication and authorization solution across on-premise and cloud environments as well as end-user devices.

Biometrics should be at least one of the factors enterprises use for enabling authentication. Unisys recommends using behavioral biometrics that can be implemented with minimal disruption. Unisys also strongly advocates the encryption of data-in-motion – even on internal networks – to mitigate the threat of packet sniffers and malicious insiders. Security incidents and events across the application landscape should be analyzed in real-time to thwart breach attempts, with mining of this data using the latest analytic techniques for forensic analysis, post breach-detection, and containment.

Federal Information Technology Governance

Overview

The pervasive use of and dependence on Information Systems by government agencies has made corresponding Information Technology budget projections rise to nearly $90 billion for fiscal year 2017. Given such large projected expenditures, examples of large IT projects that have failed abound. Among these are the FBI's Virtual Case File (a $190 million loss) and, more recently, the Healthcare.gov undertaking (a $600 million loss).

In each of these cases, the failure to perform as expected could be traced to a breakdown in the governance process. In the case of Healthcare.gov, the Government Accountability Office (GAO) found that the government "lacked effective planning or oversight practices."[2] In sum, the governance process used for this project was, at best, ineffective.

What is IT Governance?

Simply put, IT Governance is a process used to ensure that IT strategies and spending are aligned with the strategic goals and objectives of the given agency, and that a method is in place to regularly measure IT performance and ensure that stakeholder interests are considered in all IT acquisitions. This is not as simple as developing a policy, declaring that you have now instituted governance, and moving onto the next issue at hand.

The Role of the Chief Information Officer

Within the government, the need for IT Governance is made even clearer by the Clinger-Cohen Act, which formally established the Chief Information Officer (CIO) to be at the head of the IT organization and enumerated specific responsibilities for agency CIOs. These responsibilities include:

1. Alignment of IT and agency strategies;

[2] Ricardo Alonzo-Zaldivar, "Probe Finds Reasons for Obamacare Website Failure," July 31, 2014, available from Inc.com. Accessed on August 29, 2016 at http://www.inc.com/associated-press/management-failure-results-in-healthcare.gov-woes.html

2. Monitoring of IT value;
3. Efficient use of resources; and
4. Risk-management.

Agencies that have good governance processes will find that they have the internal controls needed to establish the core capabilities that comply with the law.

Government Agencies and IT Governance

So, what is a good IT governance process for government agencies? That depends on the agency, its goals, and the level of IT maturity present. Numerous, well-recognized industry standard models exist with different points of emphasis. The most popular in the industry is CoBIT, developed by the Information Systems Audit and Control Association. CoBIT is well-suited to organizations that need to focus on risk management and mitigation. The Information Technology Infrastructure Library (ITIL) is likewise widely recognized and accepted in the industry. ITIL focuses on service delivery and operational sustainability. Another framework is the Capability Maturity Model Integration (CMMI) method, created by government and industry entities working in collaboration with Carnegie-Mellon's Software Engineering Institute. CMMI is focused on process improvement and lifecycle development.

Ensuring IT Strategies Are Aligned

All of the aforementioned models are just that, models. They represent a good foundation upon which to build a sound governance system based on the needs of the agency in question. However, regardless of the model or governance system, three critical elements are necessary to ensure IT strategies and spending are successfully aligned with the strategic goals and objectives of the given agency.

First, there must be buy-in at the executive level, both within and outside of the IT organization. While the CIO oversees the IT department, there must be a clear, joint approach to IT acquisition and development throughout the agency.

Second, whatever process is followed, it must be rigorously adhered to throughout the organization in order to prevent the issues associated with “shadow IT.”

Finally, the process must be evaluated regularly to ensure that it is effective for the current situation within the agency and, if found to be ineffective, it must be changed accordingly.

Summary

The risks associated with poor governance should not be allowed to go unchallenged and uncorrected. Poor governance leaves agencies open to financial loss and a cumulative breakdown of strategic goals and objectives.

Identity and Access Management

Overview

The increasing dependency on information technology systems and networked operations pervades nearly every aspect of our society. While this dependency produces significant benefits, it also increases risk and vulnerability as sectors attempt to safeguard our nation's physical and digital assets from attacks that continue to grow in sophistication. Just as we work to protect both physical and digital assets, we see a growing convergence of physical and digital security. Unisys believes that these growing threats can be mitigated with the evolution of identity to embrace physical and behavioral biometrics, artificial intelligence analytics, and the use of distributed trust models based on blockchains.

Continuous Security and Governance, Risk, and Compliance Health

Enterprise organizations are embracing complete approaches as the next logical step in leveraging Identity and Access Management (IAM) in order to achieve and maintain continuous security as well as **Governance, Risk and Compliance** (GRC) health. Critical GRC elements include:

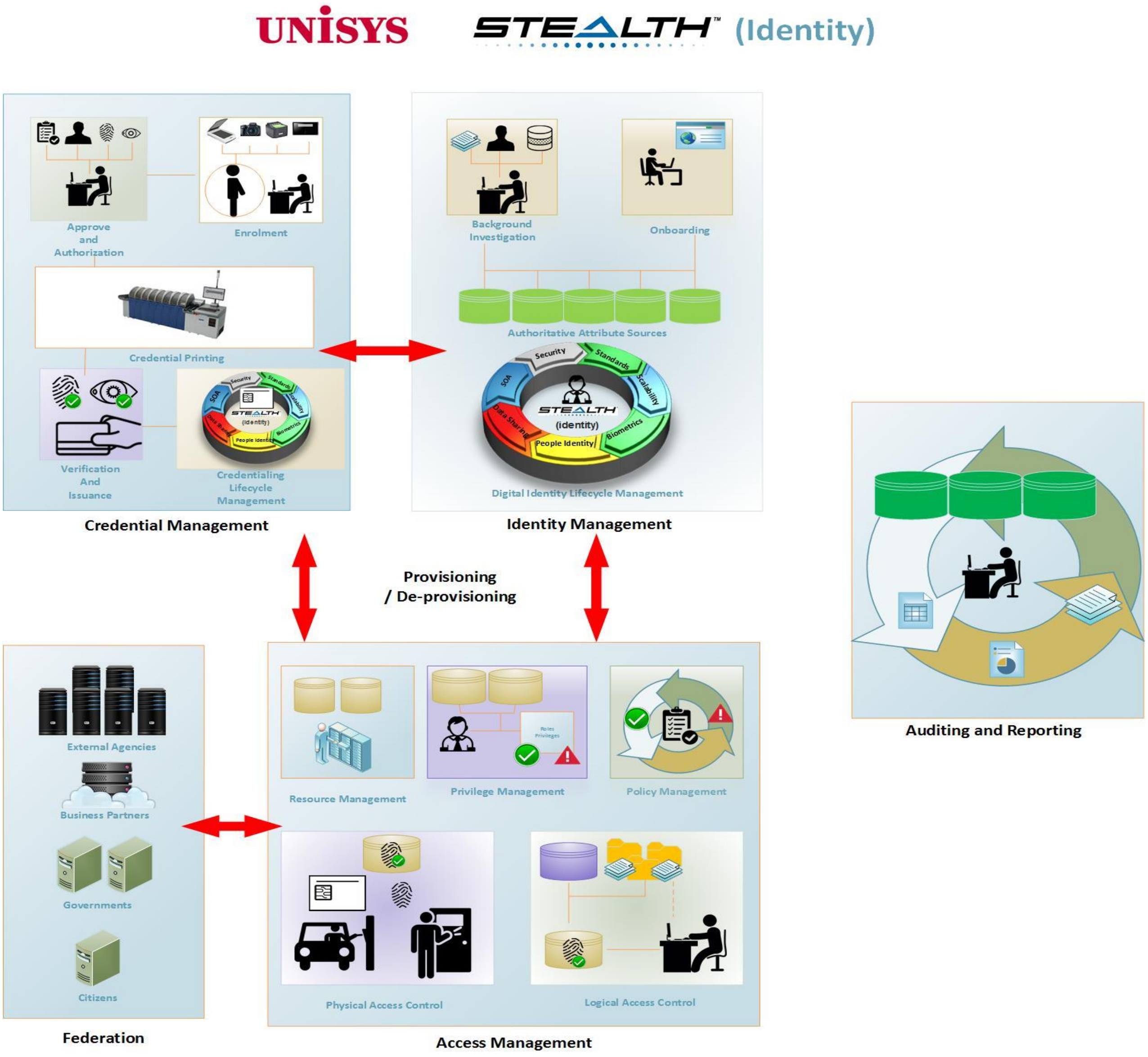
- Role-based lifecycle management
- Real-time audit and reporting capabilities, with security alerts
- Continuous policy enforcement and reporting
- Standards-based access control and automated password reset
- Automated user provisioning/de-provisioning

All of these capabilities must integrate easily with existing systems and data sources to secure businesses, support GRC initiatives, and create better business practices through IT efficiencies.

What is the IAM Framework?

Unisys recommends the use of an IAM framework that is comprised of the programs, processes, technologies, and personnel used to create trusted digital identity. Unisys sees IAM as the intersection of digital identities, credentials, and access control in one comprehensive approach. The following figure illustrates the core components of IAM.

Figure 1: ***Core Components of IAM – by example – in Unisys Stealth(identity)***



IAM is the who, what, where, when, and why of information technology. It encompasses many technologies and security practices, including secure, single sign-on (SSO), user provisioning/de-provisioning, authentication, and authorization.

Over the past several years, Forbes 2000 companies and governments worldwide have come to rely on a sound IAM platform as the foundation for their GRC strategies.

Current and Future Trends

Currently, IAM infrastructure is focused on solutions that provide:

- Policy and workflow definition;
- Documentation;
- Policy enforcement and operationalization; and
- Monitoring, testing, and verification of controls at the IT infrastructure layer.

The clear trend is one of convergence toward the enhanced use of physical and behavioral biometrics, artificial intelligence-based analytics of live video and sensor data, and the use of distributed trust models based on blockchains.

IAM is an ongoing, dynamic process. As more organizations decentralize and the consumerization of IT increases, the need for strong security and GRC practices is greater than ever. The number of highly publicized IT security breaches is growing, and with it the demand for more detailed audits and reporting requirements within organizations. This creates time-consuming challenges for IT and business professionals who are required to perform painstaking logging, reporting, and audit point processes necessary to meet standards and compliance, such as SOX and a myriad of other regulations.

These challenges extend to access control, systems integration, transparency, automation, and remediation. Without proper tools, tasks like these soon overwhelm employees, making them prone to errors and oversights.

IAM is now increasingly used in conjunction with Secure Information and Event Management (SIEM) and GRC software to provide a comprehensive and holistic approach to enterprise security and compliance. SIEM solutions include software designed to aggregate data from multiple sources in order to identify event patterns that might represent attacks, intrusions, misuse, or failure. Event correlation simplifies and speeds the monitoring of network events by consolidating alerts and error logs into a short, easy-to-understand package.

Implementing an IAM/SIEM/GRC infrastructure is not a do-it-and-forget-about-it IT process. It involves an ongoing relationship with Human Resources and business managers. After discovery has taken place, roles have been defined, and access privileges have been granted or revoked based on job function and division, transactions must be validated and certified as being in compliance with policy and regulations. Therefore, the ability to automatically pull access, control, and data usage information from various system sources and generate timely exception reports that can be matched against policy is highly appealing to most corporations.

A current trend in IAM is the concept of **Bring Your Own Device (BYOD).** Employees are encouraged to bring their own devices for use at work and are then provided tokens they can use to gain secured access to their organization's network and information. This creates a new set of security challenges.

Enterprise role management is tightly coupled with access management. It must be scalable to adapt to new organization structure and growth. As an organization evolves, roles and user groups must also be flexible to accommodate change and provide role-based access control—for both physical and logical access.

Various trends in **web authentication methods** are also emerging at a rapid pace. The use of **biometric-based**, **multi-factor authentication** is becoming very popular. It provides a secured method of authenticating an individual before access is granted. Multi-factor authentication can be carried out using biometric or non-biometric methods, such as **Out-of-Band authentication**. This is becoming particularly popular with banks.

For example, when a customer wants to make an online banking transaction, a text message is sent to the mobile phone number the bank has on file. The customer receives a one-time password that must be provided on the website in order to complete the transaction. This method has proven to be quite challenging for hackers to overcome.

The technology and solutions for cardholder provisioning from an authoritative identity source to a Physical Access Control System (PACS) have been in use for several years now. However, although the desire to implement this kind of solution has been voiced highly by organizations, the roadblock has been cost of ownership and funding.

Future trends include:

- **Scalable identity proofing** by collaborating and partnering to validate accurate online identities
- **Business enablement** with greater understanding of customer needs and an improved user experience
- **Risk-based authentication** methods devised from a user's contextual information

Other future trends include **Internet of Things** technologies as well as **cloud-based Identity and Access Management**.

Current Challenges

Of the many challenges present in identity and access management one of the most damaging is **Identity Fatigue**, where the user must provide a new user ID and password for each new application. This has been identified as a growing problem in Identity

Management. Data breaches are a common, ever-present challenge and a constant threat to cybersecurity. There must be a coordinated effort to manage and mitigate these breaches. The changing face of the threat landscape is also an ongoing challenge, since insider attacks continue to grow in number.

Progress Made

With regard to progress made, of note are **flexible authentication methods**. Progressive trends show that identity-defined security will allow for **intelligence-based**, **risk-based**, and **adaptive decision-making** in all aspects of cybersecurity as well as physical security. This type of decision-making will allow organizations to dynamically manage threats, breaches, and incidents, as well as leverage detailed reports of the entire system according to the metrics yielded by these integrations. Also promising is the emergence of Risk Engines, allowing for threats to be determined prior to their occurrence and for corrective action and mitigation to take place accordingly.

Promising Approaches

Among the most promising approaches is the emergence of **user-centric identity management,** in place of the **enterprise-centric identity management** approach. **User-centric-identity management** determines the levels of access and information the user requires to perform a service or access a facility.

Another promising approach is the convergence of physical security, logical security, and identity management into a single platform for situational awareness and management. Blended threats and insider threats can be identified by analyzing unified data from all sourced systems.

What's Next

As companies embrace newer technology to improve economies of scale and reduce operational expenses, security and compliance issues will continue to be top-of- mind for C-level executives. All areas of IAM contribute to access control and compliance, including advanced authentication, Web SSO/federated SSO (WSSO/FSSO), enterprise SSO (ESSO), user provisioning, personal portable security devices and frictionless authentication, SIEM, and access governance.

Secure access control is critical, since corporations and other entities must be able to track and report on "who had access to what, when" and what was done with data. Even if a company contracts with a cloud service provider, it is not exempt from its responsibility to comply with regulations.

Vendor success in today's market rests largely upon the building of sound partnerships and ecosystems, since an identity-driven infrastructure must be relied upon in conjunction with GRC and systems management capabilities. Again, no single entity has all the necessary pieces of the compliance and security puzzle. Furthermore, as consumerization of IT blurs the line between our professional and personal lives, risk factors multiply, making the need for holistic and proactive solutions all the more critical.

Future Challenges

An ongoing challenge we foresee extending into the future is the implementation of biometrics for authentication in logical and physical security systems. With regard to the protection of Personally Identifiable Information (PII), the use of biometrics raises concerns for organizations as well as individuals. Often, this challenge is compounded by individuals and organizations who resist change in organizational culture.

Security and Privacy Considerations of the Internet of Things

What is the Internet of Things?

The Internet of Things (IoT) refers to the enabling of everyday devices (often called "smart" devices) with network connectivity so that these can send and receive data. IoT devices are produced for both individual consumer and industrial applications. IoT changes how everyday devices are accessed, either by adding a capability that was never there before or by changing the communication method used to access these devices.

IoT is often brought to market with little regard for security and privacy. At Unisys, we focus on designing security into this category of technology as we have in all others. The size and scale of the IoT space, however, requires different tactics to accomplish proven security goals. One example of such a tactic is placing groups of IoT devices on separate segments of an enterprise network so that a breach in one area cannot affect devices in another. A second example is changing the commonly used "third-party trust" model (i.e., the use of certificate authorities) to one of distributed trust (i.e., blockchain), since the potential scale of the number of IoT devices is likely to break historic models.

An everyday consumer device, such as a smart garage door opener, can be connected to a home wireless Internet network and accessed via a smart phone, allowing the user to open and close the garage door remotely. The device can also warn the user when the garage door is left open so that the user's home is not left unsecured. In this case, the garage door opener has the added capability of using an application to provide control utilities via the Internet.

An example of an everyday industrial application of such a capability would be connecting to a remote electrical substation from a central or home-base location. In the not so distant past, this type of communication would have taken place via a low-speed serial connection and would have merely provided the user with metering. A more recent enabled capability for the same purpose would be a cellular modem with two-way communication used to both monitor and modify settings. An electric utility could, for example, adopt this capability in order to reduce the number of visits to a station, thereby saving time and money. In this case, the Internet replaces the previous communication channel and adds a new capability.

Why Does the IoT Pose Special Security and Privacy Issues?

While the IoT presents significant advantages, it also poses new security and privacy issues. Using an IoT-capable garage door opener is an added convenience for homeowners, but they would certainly not want a vulnerability that could make it possible for a burglar to gain unauthorized access to their home. A nuisance attack, such as one resulting in the homeowner's garage door ceaselessly opening and closing, would be annoying for the homeowner and embarrassing for the vendor. Nevertheless, for the homeowner, the issue could be quickly resolved by simply disconnecting the device. An industrial attack, on the other hand, would have much more serious repercussions. A hacker could very well disable a power station, causing a blackout or, worse yet, damage equipment, leaving an electric utility scrambling to address the rippling impacts on dependent systems while wasting precious time and revenue.

The privacy issues posed by the IoT have garnered a great deal of public attention. Everyday devices often gather data that can be exploited to single out user demographics and usage trends. Everyday users, for example, may hesitate to adopt new technologies that present potential privacy breaches, such as an intruder gaining access to a home-monitoring camera. The legal implications for the providers of these everyday devices must also be considered, implications that bring with them uncertainty in related markets.

How Can These Issues Be Addressed?

The key approach for addressing the range of issues associated with the IoT – be it in the industrial or everyday consumer context – is establishing robust situational awareness. This situational awareness can take a number of forms. For example:

- Awareness of the consequences resulting from the compromising of different classes of everyday devices and their uses
- Awareness of the technical deployment of these devices
- Awareness of potential threats to these devices

Consequence Awareness

For industrial applications, a scalable assessment of potential repercussions for individual installations can be performed to guide mitigation planning. For everyday consumer applications, generic consequence assessments can be performed in order to provide guidance to vendors, integrators, and other consumers. At a national level, ongoing research on interdependencies, such as that conducted by *Peerenboom et al* at Argonne National Labs in 2001, can further clarify resource allocation as well as legislative and regulatory priorities at the public and sector levels.

Technical Awareness

Appropriate deployment of monitoring processes and technologies in IoT installations can provide detection of malicious and non-malicious failure modes, enabling effective mitigations. In some large industrial installations, these processes and technologies can be managed by asset owners and operators with support from their suppliers. In the majority of industrial installations, and all consumer applications of IoT, vendors, integrators, and service providers can offer scalable and economically viable solutions to monitor the systems that utilize IoT technologies.

Threat Awareness

Threat Intelligence systems and technologies have advanced significantly over the past decade. It is now possible to engineer national and global intelligence-sharing networks that transport pertinent IoT applications intelligence to relevant parties. Where **Consequence Awareness** and **Technical Awareness** are present within the industrial and consumer applications of IoT technologies, actionable threat intelligence can be effectively applied to mitigate or limit the impact of malicious, as well as non-malicious, isolated, or cascading failure modes. Vendors, integrators, and service providers are currently integrating threat intelligence capabilities into products, architectures, and services.

Summary

The IoT presents both strategic advantages as well as new risks to infrastructure and the public. It is likely that it will continue to be infeasible to address the aforementioned risks entirely through efforts to produce devices and systems that are immune to malicious and non-malicious failure modes. Yet, it is entirely feasible and economically viable to engineer systems and supporting technical and business infrastructures that enable safe and resilient operations by implementing situational awareness. Technical capabilities, business processes, and public sector efforts already in place can advance and deliver this situational awareness infrastructure with the continued pursuit of existing development directions.

Unisys possesses the history, skills, and scale to work with the government as well as private sector stakeholders to advance situational awareness capabilities pertinent to the IoT. Unisys' global constellation of **Security Operations Centers** provides mature **Managed Security Services** that already deliver **Threat Awareness** and **Technical Awareness** to enterprises around the world. Unisys makes scalable **Consequence-Based Assessments** possible in order to help organizations allocate human and economic resources appropriately. The scale and range of Unisys’ capabilities permit enterprises to execute a security strategy that is appropriate to their role in the IoT.

Public Awareness and Education

Background

In both the near and long-term future, industry experts agree, the need for cybersecurity as well as the means to defeat cybercriminals and the threats they represent will be on the rise. Recent industry reports show a 458 percent increase in the number of hackers who prowl the Internet for vulnerabilities.[3] This prowling has caused malware attacks to nearly double – with Android ecosystems being the prime target.[4] In just over the past year, an increase of 55 percent has been observed in the incidence of spear-phishing campaigns that target employees.[5] Additional estimates suggest that, by 2019, the cost of data breaches to business will increase to $2.1 trillion; that is, by four times the cost of those in 2015.[6]

Effective cybersecurity is akin to neighborhood-watch programs, which have proven to be effective only when neighbors are educated and willing/active participants who monitor, report, and support law enforcement in its efforts to do away with perpetrators.

Preparedness Expertise and Philosophy

Meeting the challenge set by the National Institute of Standards and Technology (NIST) to create and maintain a coherent as well as comprehensive public awareness and education program – one that enhances partnership coordination and cooperation – requires experience and proven innovations. A seasoned cybersecurity industry leader,

[3] AT&T, "What Every CEO Needs to Know About Cyber Security: Decoding the Adversary," *AT&T Cybersecurity Insights*, Vol. 1, 2015, p. 6. Accessed August 30, 2016 at https://www.business.att.com/content/src/csi/decodingtheadversary.pdf

[4] Dell, "Dell Annual Threat Report Reveals Cyber Criminals Using Aggressive, Shape-Shifting Threat Tactics; 50% Surge in Encrypted Traffic Affected Millions of Users in 2015," February 22, 2016, p. 1. Accessed August 30, 2016 at http://www.dell.com/learn/us/en/uscorp1/press-releases/2016-02-22-annual-threat-report-details-the-cybercrime-trends

[5] Symantec, *Internet Security Threat Report*, Vol. 21, April 2016, pp. 6-9. Accessed on August 30, 2016 at https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

[6] Juniper Research, "Cybercrime and the Internet of Things," May 12, 2015, p. 6. Accessed on August 30, 2016 at http://www.juniperresearch.com/document-library/white-papers/cybercrime-the-internet-of-threats

Unisys holds the strategy and solutions that harness effective public awareness and education across both the private and public sectors. As part of its **Protect-Detect-Respond-Remediate** cybersecurity philosophy, Unisys stands apart. Unisys offers industry-leading technology and expertise from across a wide range of global, cyber-industry experiences and solutions. Thus, Unisys delivers integrated cybersecurity public awareness and education solutions for some of the most demanding challenges that government and Fortune 500 companies can face.

Public Awareness Strategy and Methodology

Unisys offers experience in the latest technical guideline development, cyber resiliency, and information and privacy consulting concerns. These are essential for both in-house and managed services activities that support public awareness through the cyber incident response crisis cycle. Unisys' strategy is focused on the development and integration of internal program support and external collaboration to address essential issues, provide critical feedback, and establish a presence that provides for the most compelling education messaging for user-communities.

Public awareness and education is critical in preparing user-ready communities who can successfully mitigate the attempts of current and emerging threats to breach their systems and destroy their operating capabilities. The capacity to detect and understand new and emerging threats, as well as determine and create the solutions and education programs needed to quickly mitigate them, can mean the difference between success and failure.

Within its **City Event Readiness** methodology, Unisys holds the solutions development and technology/architecture assessment capabilities that tie together the necessary:

- Conventional as well as social media threat management support;
- Policy and technology enforcement;
- Technology and incident response;

- Event program management; and
- Concept of Operations execution.

Together, these ensure user-community preparedness.

Effecting Change and Enhancing Readiness

As new technology applications emerge, so do attacks. Readiness to defeat emerging and future threats, as well as to mitigate the related risks that constitute these, depends on appropriately trained and effective teams who are knowledgeable and competent in their capabilities.

Protecting the safety and security of critical cyber operations and cyber systems, while creating public awareness, requires teams who are adequately prepared to mitigate quickly developing threats and risks. Unisys relies on its unique blend of **Consequence-Based Assessments** (CBA) and **Wargaming** capabilities to evaluate team readiness and identify actionable recommendations.

What is Wargaming?

At its core, Wargaming is based on the Department of Defense's time-tested procedures and Unisys' commercial best business practices. Wargames assess client's internal and external strategic risks across the spectrum of logical and physical security environments. This includes Critical Information, Physical Protection, Operating System, Information Access, and External Access.

Wargaming assesses cyber incident response, resolution, decision-making, and coordination of processes and capabilities. Unisys' Wargames – tailored to a client's specific needs – may include a simulated "attack" to test security staff and systems and incident response management. With the use of a free play, an interactive Red Team challenges solution effectiveness – and their implications – and identifies risks derived from unforeseen threat actions. A Green Team serves to adjust goods or services provided to the client and replicates competitor responses to solutions.

Unisys’ Wargames also test internal and external communications (including communications with customers, investors, financial institutions, and the supply chain) across all media, including Social Media.

Unisys’ Wargames deliver a detailed findings report comprised of observations, insights, and actionable recommendations regarding improvement, sustainment, development of new processes and capabilities, and the allocation of resources to address emerging risk. Client benefits include reduced business risk, decreased downtime, improved competitive advantage, improved profitability, enhanced brand recognition, and improved customer satisfaction.

Cybersecurity Trends

Overview

Today's data breaches and the headaches associated with them concern companies the world over. This year, after a close examination of more than 2,100 of these breaches, one such company concluded that "no locale, industry, or organization is bulletproof when it comes to the compromise of data."[7] There is, however, cause for hope. The Cybersecurity Industry is always rapidly evolving to keep pace with ever-emerging threats, methodologies, and actors. Five new trends aim to tackle these challenges.

From House to Hotel: Rethinking Perimeter Security

In the past, cyber defense has had a perimeter focus, similar to the attention homeowners give their home when attempting to secure it. They lock windows and doors and install an alarm or intrusion prevention system. With a primary focus on the exterior perimeter, the internal infrastructure is left open to other vulnerabilities.

To this point, the issue of whether or not an intruder will breach an outer perimeter is more a question of "when" rather than "if." In 84 percent of breach attempt incidents, it took intruders less than 24 hours to break through exterior perimeters,[8] leaving them free to run laterally within a network.

Microsegmentation – a Gartner top 10 security technology for 2016 – acts more like a hotel, creating cryptographically controlled micro perimeters, while granting access based on the user's identity.

[7] Verizon, "Data Breach Investigations Report," 2016. Accessed August 30, 2016 at http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

[8] Verizon, "Data Breach Investigations Report," 2016. Accessed August 30, 2016 at http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

Killing the Password

Phishing, and its tandem trend, "whaling," continues to be an effective strategy for compromising networks. (Whaling refers to socially-engineering a phishing attack to resemble a credentialed person of importance within a company attempting to gain access.) Relying on static credentials, username and password, creates a risk that is dependent upon humans to maintain control over access.

Recently, a global survey that aimed to shed light on the security practices of company employees, determined that, when given the chance, 28 percent of U.S. respondents would sell their corporate username and password,[9] sometimes for less than 100 dollars.

The implementation of two-factor authentication and biometrics helps add a layer of security that goes beyond passwords, which can be cracked or compromised.

Big Data, Analytics, and Artificial Intelligence

The human factor poses primary risks, such as in the case of static credentials. Cybersecurity technologies that leverage big data, analytics, and artificial intelligence take the biology out of the equation to focus on the binary. Most especially, the analysis of:

- Attack patterns;
- Application and communication behavior; and
- Proactive sandboxing

helps deliver an advanced look at threats *before* they can infect, spread through, or fully compromise a network.

Reaching Across the Table: The Role of Partnerships

The fabric of the Internet is one of borderless anonymity and, as such, often makes it possible for attackers working at computers halfway around the world to remain unseen.

[9] SailPoint Technologies, Inc., "Identity Governance Market Pulse Survey," 2016. Accessed August 30, 3016 at https://www.sailpoint.com/identity-governance-market-pulse-survey/

Hacktivists, as well as well-funded nation-state attackers, make for challenging adversaries. Critical in this landscape are partnerships between agencies, states, and governments to share vital information on cyberattacks and develop new methodologies. A joint effort is critical to a proper cyber defense strategy. Such agencies as the National Cyber Security Alliance and the Cyber Security Research Alliance seek to bring together industry leaders, companies, and organizations to share effective strategies, best practices, and expert insight.

Developing a Cybersecurity Workforce

Recently, the IT Market research firm ESG determined that 28 percent of organizations are facing a problematic cybersecurity skills shortage in their personnel. ESG's finding sheds light on how critical it is to foster the expertise necessary for employees to defend against threats in an always-evolving security landscape. Of note on this front is Cisco's attempt to help bridge the skills gap by launching a $10 million cybersecurity scholarship fund. Universities around the globe are now instituting security-specific tracks in their CIS programs.

Summary

The benefits of constant connectivity will likely always present tandem risks. However, new trends to temper those risks and defend against threats are always emerging, making it possible for companies to have the tools they need to help them keep pace.

Contributors

Chris Blask, Global Director, Industrial Control Systems (ICS), has served in the ICS and information security industries for more than 25 years. Throughout a career that spans the breadth of the cybersecurity spectrum, he is credited with inventing one of the first commercial firewall products, building a billion-dollar firewall business at Cisco Systems, co-founding an early SIEM vendor, and authoring the first book on SIEM. He serves as Chair of the Industrial Control System Information Sharing and Analysis Center (ICS-ISAC) and as Chair of the International Association of Certified ISAOs (IACI).

John Bone, Global Director, Wargaming and Exercises, served in the U.S. Army for 27 years, retiring as a Colonel, during which time he developed expertise in crisis management and led servicemen and women in the conduct of high-risk special operations, with direct responsibility for 150-plus person War Games for NATO and all three U.S. military services. For six years, Bone led the Irregular Warfare War Game capability as well as capacity development efforts at the Joint Forces Command J9 Directorate and served as Chief of the Joint Irregular Warfare Center's War Gaming practice. He is an expert in the planning, preparation, and conduct of War Games, simulations, and tabletop exercises.

Scott E. Clark, Senior Cyber Security Architect for Security Services, has over 30 years of defense contracting and U.S. Army experience. He designed and delivered wargames, exercises, and capabilities developments across the U.S. government and the private sector. His efforts include supporting the U.S. Army wargame series "Unified Quest" and the NATO Countering Hybrid Threats strategic concept wargame. He has also designed crisis response and cyber incident wargames for the United States Postal Service, as well as commercial banking and financial institutions. A 20-year U.S. Army veteran, Clark's assignments have included United States, Europe, and the Middle East.

Dhimant Desai, Global Lead, Physical Security Solutions Portfolio, has been with Unisys for 32 years, 20 of which he has spent working in Identity Management. He is a recognized Biometrics subject matter expert, known for having deployed dozens of large scale biometrics-based Identity projects worldwide. He also serves as Product Manager for the state-of-the-art Stealth(identity) framework.

Edward J. Liebig, Vice President, Global Security Services, has over 37 years of IT experience. His areas of expertise include executive security program management, strategic and tactical security project management and operations, IT and ICS governance, full secure lifecycle management, application development, internal and external audit, regulatory compliance, and controls assurance. He has served as CISO for major multinational corporations. Liebig has amassed and led broadly skilled technical teams to build out and sustain comprehensive security programs for numerous companies in a wide range of industry verticals with a keen focus on Critical Infrastructure, including Chemical, Energy and Natural Resources, Manufacturing, Financial Services, Retail, Telecommunications, and Health Care.

Tom Patterson, Chief Trust Officer and Vice President of Global Security, leads Unisys' physical and logical security practices. In this role, Patterson directs a global team helping clients deploy and operate the most appropriate security countermeasures to include supporting cybersecurity for high-profile events, such as Super Bowl 50. A proven security leader, Patterson has been working for three decades on all facets of cybersecurity including hardware, software, managed services, policy, privacy, threat mitigation, compliance, and governance. Initially trained by the intelligence community, Patterdon has been named a *2016 Top Thought Leader in Trust*, is the author of a well-reviewed book, and makes regular television guest expert appearances. Patterson has also advised the White House, the FBI, USSS, and NCIX on cyber issues and activities, and continues to work closely with the Fort Gordon Alliance to maximize the success of Cyber Command and related DoD and IC cyber activities.

Stuart Phillips, Senior Program Manager for Industrial Control Systems, brings over 25 years of experience in Security, Networking, and Unified Communications. Having worked with such large vendors as Cisco, Polycom, and Avaya, Phillips has extensive experience with end-users in the military, government, and financial markets. He is responsible for founding and managing a sub-contractor for the U.S. Air Force via Lockheed Martin to develop software models for highly degraded satellite networks. Phillips holds a Bachelor's Degree in Computer Science and a Master's Degree in Business Administration.

Rod Sapp, Vice President, Global Security Product Management, is responsible for Unisys security product strategy, the security product's operating and investment plans, and the management of the product lifecycle. Sapp has spent the past six years overseeing the development and commercialization of the award-winning Stealth advanced security and micro-segmentation product. He holds a Bachelor's Degree in Management Science and a Master's Degree in Business Administration from West Virginia University.

Bill Searcy, **Vice President, Global Justice, Law Enforcement, and Border Security Solutions**, has been with Unisys since his retirement from the Federal Bureau of Investigation (FBI). While serving as the FBI's Deputy Assistant Director of the IT Infrastructure Division, Searcy was responsible for the engineering, development, deployment, maintenance, and security of the FBI's worldwide IT infrastructure. In this role, he was responsible for numerous modernization initiatives, among them, the development and deployment of the Enterprise Remote Access System. Previous roles at the FBI included serving as the Chief of the Cryptologic and Electronic Analysis Unit and as Chief of the Data Acquisition/Intercept Section.

Scott Spiker, **Global Business Development, Cloud Security Director**, provides technical assistance to organizations throughout the West on developing cybersecurity strategies and systems that take advantage of the economic benefits of the public cloud. His career began with Symantec. He joined Unisys in 2015 to help global companies extend their datacenter workloads securely into the cloud.

References

Alonzo-Zaldivar, Ricardo. “Probe Finds Reasons for Obamacare Website Failure.” Inc.com. July 31, 2014. Available from http://www.inc.com/associated-press/management-failure-results-in-healthcare.gov-woes.html, accessed August 29, 2016.

AT&T. “What Every CEO Needs to Know About Cyber Security: Decoding the Adversary.” *AT&T Cybersecurity Insights*. 2015. Available from https://www.business.att.com/content/src/csi/decodingtheadversary.pdf, accessed August 30, 2016.

Byrne, Donald. “Consequence-Based Analysis: An Emerging Risk Assessment Paradigm.” *LawPracticeTODAY*. April 2011. Available from https://www.americanbar.org/publications/law_practice_today_home/law_practice_today_archive/april11/consequence-based_analysis.html, accessed September 7, 2016.

Dell. “Dell Annual Threat Report Reveals Cyber Criminals Using Aggressive, Shape-Shifting Threat Tactics; 50% Surge in Encrypted Traffic Affected Millions of Users in 2015.” Dell press release, February 22, 2016, on the Dell website, http://www.dell.com/learn/us/en/uscorp1/press-releases/2016-02-22-annual-threat-report-details-the-cybercrime-trends, accessed August 30, 2016.

Juniper Research. “Cybercrime and the Internet of Things.” May 12, 2015. Available from http://www.juniperresearch.com/document-library/white-papers/cybercrime-the-internet-of-threats, accessed August 30, 2016.

SailPoint Technologies, Inc. “Identity Governance Market Pulse Survey.” 2016. Available from https://www.sailpoint.com/identity-governance-market-pulse-survey/, accessed August 30, 3016.

Symantec. *Internet Security Threat Report*. Vol. 21, April 2016. Available from https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf, accessed August 30, 2016.

Verizon. “Data Breach Investigations Report,” 2016. Available from http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/, accessed August 30, 2016.