Redbooks
ibm.com/redbooks

Industrial Controls Security

James Eaton

Craig E Heilmann

Anja Jessica Paessler

Simone Riccetti

Rick Robinson

Security

IBM

Redguide

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

This document, REDP-5323-00, was created or updated on January 5, 2016.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

IBM®
PureSystems®
QRadar®
Redbooks®
Redguide™
Redbooks (logo) ®
X-Force®

The following terms are trademarks of other companies:

Adobe, the Adobe logo, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Java, and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Other company, product, or service names may be trademarks or service marks of others.

Executive overview

When the topic of IT security came up, people used to immediately think of antivirus software, firewalls, and other logical and physical security measures. Stuxnet,[1] data thefts, and other cyberattacks against government institutions and corporate organizations are indications that the security landscape is rapidly changing. Our world has become increasingly digitized and interconnected, which only increases the opportunities for attackers to harm our organizations and our way of life. These days, attackers are organized and well-funded. As cybersecurity threats evolve, we must adapt the way to fight them. The typical countermeasures are no longer adequate, given that advanced persistent threats (APTs) are the most imminent attacks that we face today.

This IBM® Redguide™ publication explains why industrial installations are an attractive target and why it is so important to protect them in a new way. To help you better understand what you might be facing, we explain how attacks work, who the potential attackers are, what they want to achieve, and how they work to achieve it. We give you insights into a world that seems like science fiction but is today's reality and a reality that threatens your organization. We also show you how to fight back and explain how IBM can help shield your organization from harm.

Our goal is for you to understand what the current threat landscape looks like and what you can do to protect your assets.

The seriousness of IT vulnerabilities

Imagine what could happen if someone penetrated your IT or industrial system and gained access to personal data, client data, proprietary business information, research and development, or code in your production facilities. What can happen if your data were to be maliciously used by external parties, competitors, or an entity that used your compromised assets to their advantage? Imagine that a malicious intruder could control your IT or production environment by accessing your Supervisory Control and Data Acquisition (SCADA) systems, Programmable Logic Controls (PLCs), or other industrial control systems. It could be disastrous.

[1] The Stuxnet attack was based on a computer worm that infected at least 14 industrial sites, including a uranium enrichment plant. See *An Unprecedented Look at Stuxnet, the World's First Digital Weapon* at http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

Most people believe attacks originate outside of an organization's IT perimeter. The truth is, most security threats are not initiated as external attacks but as internal ones. This does not mean that these attacks are carried out by disgruntled or malicious employees; rather, these are external attackers who manage to get access to IT assets inside of your organization's perimeter by means of social engineering, such as phishing emails.

Actually, insider threats continue to hold a top place in comparison to other attack vectors. Outsiders were found to be responsible for 45 percent of the attacks reported in 2014. Those who had insider access to organizations' systems carried out 55 percent of attacks.[2] Modern IT trends, including the rise of social media, mobility, bring-your-own-device (BYOD) policies, the cloud, and the era of big data make threats from employees, contractors, partners, and others with trusted access harder to identify and give insiders more ways to pass protected information with a reduced chance of discovery.

But what does that mean? The term *insider threat* has multiple meanings, from a malicious employee who intentionally wants to do harm, to users who inadvertently click a suspicious email attachment and unknowingly expose their system and possibly the corporate network, to malware and an external threat. Because social engineering has become more sophisticated, it is more difficult to recognize attacks for what they are, and even the best security system in the world cannot prevent outsiders from accessing your systems if your employees are lured into a trap and you are not using the latest fraud prevention technology. Figure 1 provides more information about the top security threats.[3]

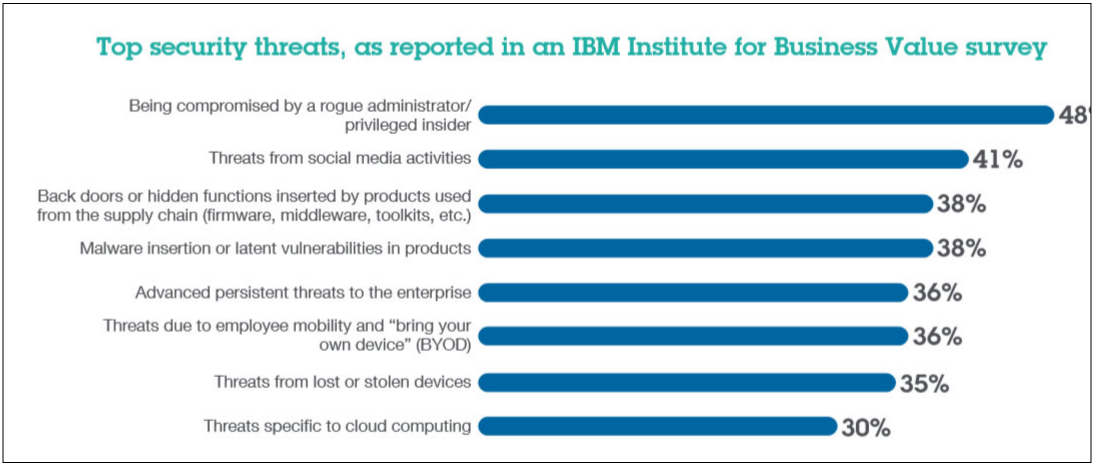


Figure 1 Top security threats according to an IBM survey

Ecosystems and supply chains are most vulnerable

Today, the ecosystem of business partners, vendors, contractors, suppliers, and their ecosystems are all connected in a global economy. Conventional security models and architectures are based on trust, identity, and access permissions, but it is getting difficult to determine how far outside of your organization that trust can and should extend.

For example, energy and utility businesses depend on the ability to control plants, substations, and other assets on the grid. Traditionally, this was carried out by using dedicated control equipment with data exchanged through stand-alone networks. The

[2] *IBM X-Force Threat Intelligence Quarterly*, 4Q 2015, "*How can your organization better prepare for a security incident?*" `http://www.ibm.com/security/xforce/downloads.html`

[3] Top security threats as reported in an IBM Institute for Business Value survey, Source: IBM Institute for Business Value, IT Infrastructure Study, Q7: How concerned are you about the following security threats? `http://www.ibm.com/at/businessconnect/assets/files/Security-XForce_Report.pdf`

isolation of such systems meant that they were relatively resistant to hacking and malware infections. Parallels can be found in other industry sectors also.

The Internet has changed all of this. Rather than using dedicated networks and protocols, operators are increasingly opting for the ubiquitous, low-cost connectivity offered by the Internet. This is attractive for the energy industry because it operates enormous amounts of remote equipment scattered across large areas. Individual devices can be controlled, and the associated software can be upgraded from anywhere. The disadvantage, of course, is that security is often weak, if not altogether absent. Potentially, anyone can remotely access systems and devices that rely on Internet connectivity.

Why industrial installations are such attractive targets

According to research by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT),[4] the manufacturing sector was the target of more than 65% of reported cyberattacks in 2014. Industrial Control Systems (ICS) are the focus of these attacks, and the use of the Internet for ease of management and control has exposed them to new attack vectors.

However, new modes of operation add new risks. As the number of infrastructures increases, including millions of Advanced Metering Infrastructure (AMI) installations in the U.S. alone, and rising, so do potential points of failure. This risk is amplified as the industry continues to expand to renewables and distributed generation.

Imagine what might happen if attackers gained control over traffic control systems, programmable logic controller (PLCs), or even supervisory control and data acquisition (SCADA) systems. Power supplies might be at risk. Healthcare, commercial activities, and personal transit can come to a standstill. Supply chains might be broken, and the availability of food and water supplies could be at risk. Although this is a radical scenario, it is not impossible if critical infrastructures are maliciously attacked.

A 2010 news report[5] describes an Iranian uranium processing and refining plant that was attacked by an advanced, innovative computer malware named Stuxnet. Stuxnet has been hailed as significant for many reasons, not the least of which is that it is an example of what happens when military-grade technology is released to the public domain: It gets analyzed, dissected, and studied in great detail by malware developers. Inevitably, whatever was weaponized now becomes public knowledge and serves as the blueprint for even more advanced attack techniques used in the mainstream. For this reason, Stuxnet is particularly relevant as we gain an understanding of how to fight the fight today, because this transfer of military grade technology to the mainstream will probably continue to occur.

Another example is Citadel, which started as financial malware. Citadel has undergone a wide range of significant changes, including these examples:

- Evolving methods of stealing data, from using simple key logging capabilities to deploying fully automatic crimeware that is capable of taking over devices and capturing data and credentials
- Distribution and delivery of malware to targeted devices
- Introduction of what are called “security updates” that allow malware to evade detection

[4] *ICS-CERT Year in Review*, 2014. U.S. Department of Homeland Security, National Cybersecurity and Communications Integration Center, page 6
https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2014_Final.pdf

[5] *An Unprecedented Look at Stuxnet, the World’s First Digital Weapon*
http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

- Changing the type of target

In the past, several variants of financial malware have targeted nonfinancial institutions, including commerce web sites, airlines, hotels, healthcare organizations, and online gaming companies. The list has expanded further. A variant of Citadel now targets petrochemical sellers and suppliers and password management software, all with the apparent goal of giving attackers access to sensitive corporate intellectual properties. Citadel was also used to circumvent a two-factor authentication security system and hack into the virtual private network (VPN) of a major international airport.[6]

Citadel is a follow-up of Zeus, the financial malware that stood above all others when financial malware emerged. The Zeus source code was leaked in a Russian underground forum. That enabled cyber criminals to develop their own variants and essentially eliminate the need to buy the malware from the sellers.

This leak also offered cyber criminals a new advanced tool, encompassing what appeared to be classic Zeus capabilities along with new features. The original post in the forum indicated that the malware was Zeus-compatible, meaning that configuration files and HTML injections that were used with older versions of Zeus can work with Citadel. The advertisement highlighted that Citadel enabled the attacker to run shell commands from the infected device. This allows an attacker to, among other things, map the network in which the device was infected, thereby aiming for more than financial data.

In addition to these capabilities, purchasers of Citadel were able to influence future versions by participating in polls that the Citadel team initiated. These polls asked users to choose among features that they want to see in upcoming versions. When a feature received a majority vote and a minimal required amount of money, the Citadel team committed to developing the feature.[7]

Both the Citadel and Stuxnet cases illustrate how underground forums give attackers the opportunity to take existing source code and adjust or improve it to meet their needs. This has led to the remarkable increase in the speed and sophistication of attacks.

But why are industrial installations such an attractive target, and who is behind the attacks?

Let’s start with the first question. We already talked about the power someone has after managing to access your systems. Usuall,y the goal isn’t just to create chaos. Attacks are about competitive advantages, national security, and, of course, money.

There are many ways to benefit financially from a cyberattack. Leaked records can be sold for large sums of money, Distributed Denial of Service (DDoS) attacks that make your server or application unreachable for customers can lead to huge financial losses and benefit competitors, and if someone gains insights into your business and development plans, your organization might suffer long-lasting damage. Sometimes, we even see a more idealistic motivation behind attacks in which attackers consider themselves the good guys who fight the system, injustice, capitalism, or whatever seems worth fighting for to them.

Take a look at the bar charts in Figure 2 and see which sectors are targeted in what way.

[6] “Airport VPN hacked using Citadel malware,” *SC Magazine*. August 12, 2014. http://www.scmagazine.com/airport-vpn-hacked-using-citadel-malware/article/254604/

[7] *2015 2Q IBM X-Force Threat Intelligence Report* http://www.ibm.com/security/xforce/downloads.html

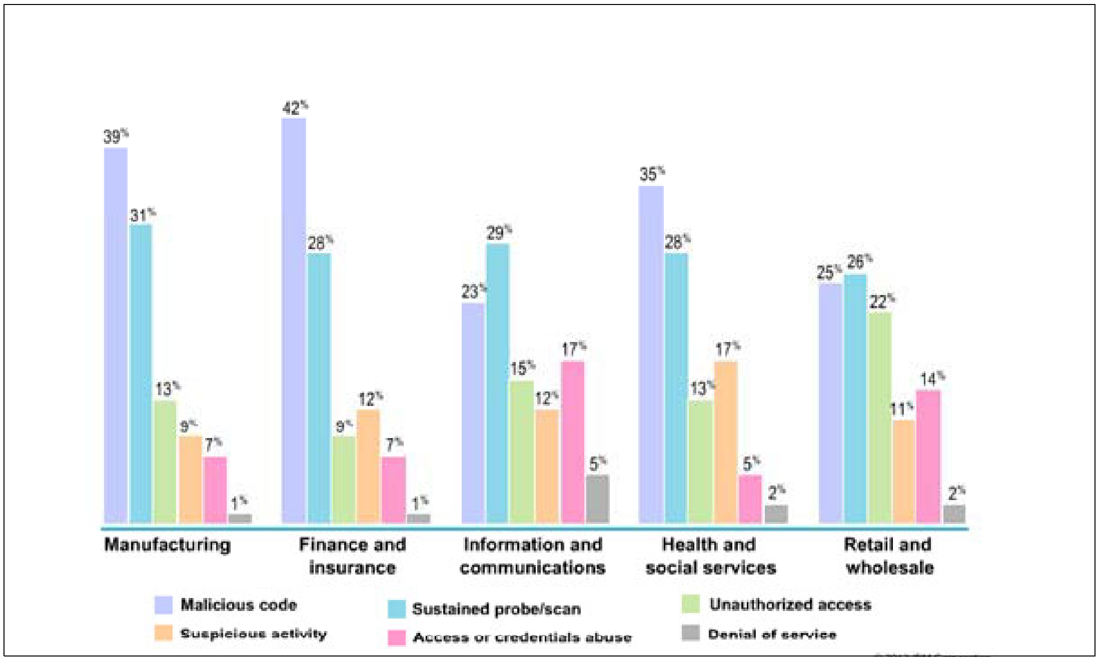


Figure 2 Attack distribution by industry

Attackers and attacks have changed over time. In the early 1990s, curious high school teenagers and clever college students (amateurs known as *Script Kiddies*) instigated most of the security incidents that were reported by the media. Over time, attackers evolved to include disgruntled employees, intellectual property thieves, and petty criminals. Then, organized crime, businesses, and individuals got involved who were motivated by money to acquire information assets. As more sophisticated actors got involved, they brought with them more resources and capabilities. Consequently, the speed, volume, and sophistication of the attacks increased and at a faster pace than the typical organization can evolve defenses.

With the evolution of these attacks in mind, consider the types of attackers, motivations, and sources that we currently face:

Opportunists Anyone, from an individual to a full-fledged nation state, that seeks to profit from the sale of their expertise, malware, access, or information (such as stolen credentials). This includes insiders who want to profit anonymously from the sale of inside information or access.

Hacktivists Ideological hackers, including individuals and groups motivated by political, religious, social, or environmental agendas. Such threat agents are more likely to want to leave their mark or make a point, rather than steal information or money. The reasons for the attacks are not always clear. The attacks can be motivated by general disaffection rather than a desire to achieve any concrete objective.

State-sponsored hackers This group is likely to encompass APTs and well-resourced attacks. State-sponsored hacking cannot be deterred easily, and it can persist for years by using different attack vectors.

Industrial rivals

Unscrupulous businesses can now enlist the help of professional hackers to launch attacks on competitors. The existence of shadowy hacker-for-hire groups means that this is now relatively easy. Attacks are used to steal commercially sensitive operational and planning data or to disrupt normal operations by sabotage.

Insiders

The people best placed to attack your organization are those closest to it. These include joint venture partners, contractors, suppliers, disgruntled former employees, and even seemingly trustworthy IT staff members. The range of motives is wide and includes espionage, extortion, and revenge.

Organized crime

Criminals' motives include stealing valuable commercial information that can be sold or obtaining money through extortion. As with industrial rivals, organized crime groups can recruit and pay for specialist hacking skills, which can be obtained online with relative ease.

Recreational hackers

These include digital troublemakers who hack organizations just because they can or because they want to impress friends or peers. Some, such as black-hat hackers LulzSec, say they hack for entertainment. In other cases, however, nuisance attacks can be carried out by Script Kiddies (youths who lack the motivation and skills needed to launch damaging or sustained attacks).

Accidental infection

Not every attack is targeted. Malware is rampant, and infection is a constant threat. Malicious software can find its way into systems by accident, either by way of the Internet or through removable media, such as Universal Serial Bus (USB) sticks and disks, or by temporary modem connections.

All of this information leads to the question: How real is the threat?

Let's follow a timeline of real-world events:

- August 2011: Operation Shady RAT is uncovered. It's a five-year campaign of targeted intrusions by a single group. For details, see *Revealed: Operation Shady RAT,* A McAfee white paper by Dmitri Alperovitch, 2011:

  http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf

- April 2012: The U.S. Department of Homeland Security identifies cyber intrusions targeting natural gas pipeline sector companies. For details, see *Gas Pipeline Cyber Intrusion Campaign,* ICS-CERT Monthly Monitor, April 2012:

  http://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Apr2012.pdf

- September 2012: Attackers install malicious software and steal project files related to OASyS SCADA, a product that helps energy firms integrate older IT assets with advanced smart grid technologies and a key offering of Telvent Canada Ltd. For details, see "Maker of smart-grid control software hacked," *Wired* magazine, September 26, 2012:

  http://www.wired.com/2012/09/scada-vendor-telvent-hacked/

- December 2012: Saudi Aramco, the world's largest oil producer, confirms that a Shamoon cyber virus attack earlier in the year was intended to stop the flow of oil and gas to local and international markets. For details, see "Aramco cyber attack targeted production," *Financial Times*, December 10, 2012:

  http://www.ft.com/intl/cms/s/0/5f313ab6-42da-11e2-a4e4-00144feabdc0.html

- May 2013: Iranian-backed hackers escalate cyber assaults against U.S. oil and gas corporations. For details, see *Anonymous Message: #OpPetrol,* June 20, 2013:

  http://www.youtube.com/watch?v=Ko_TQ_skYCY

- April 2014: Hackers shut down a floating oil rig by tilting it. For details, see "All at sea: global shipping fleet exposed to hacking threat*,"* Reuters, April 23, 2014:

  http://www.reuters.com/article/2014/04/23/us-cybersecurity-shipping-idUSBREA3M20820140423

- June 2014: The Havex remote access Trojan (RAT) is used in cyber espionage operations aimed at industrial control systems. For details, see "Attackers Using Havex RAT Against Industrial Control Systems," *Security Week*, June 24, 2014:

  http://www.securityweek.com/attackers-using-havex-rat-against-industrial-control-systems

- June 2014: Cybersecurity researchers reveal that Russian hackers have been systematically targeting hundreds of Western oil and gas companies. For details, see "Russian Hackers Targeting Oil and Gas Companies," N*ew York Times*, June 30, 2014:

  http://www.nytimes.com/2014/07/01/technology/energy-sector-faces-attacks-from-hackers-in-russia.html?_r=0

What attacks look like and how they work

Before we go a little more into detail, let's talk about what forms these attacks can take. They fall into two broad categories:

- Sabotage

  Cyberattacks can be used to reach and disrupt operations that rely on electronic control systems. In the context of energy, for example, this includes everything from distribution automation and smart grid to generation plants. For an industry that deals primarily with electrical energy availability, the dangers posed by sabotage are clear.

  Large-scale attacks are a concern for both the energy sector and for governments. But acts of sabotage do not have to be spectacular to be damaging. A significant proportion of generation in the energy industry is linked to high-volume, continuous processes: Operations that for practical and economic reasons must operate around the clock. Even low-level interference in complex processes of this sort can lead to painful losses that never make the headlines.

  The risk of sabotage continues to grow. The number of successful cyberattacks against SCADA systems at power generation plants, petroleum production plants, nuclear energy plants, and water treatment facilities has risen over the years. In 2012, ICS-CERT, part of the US Department of Homeland Security, responded to nearly 200 cyber incidents that targeted control systems. More than 40% of the attacks were directed against the energy sector, including a *spearphishing*[8] campaign to obtain data to use to facilitate unauthorized operations by using ICS and SCADA systems. By 2013, this malicious type of activity had risen to 56%.

[8] Spearphishing occurs when targeted email messages request access details, contain contaminated attachments, or link to the phisher's web page.

- Data theft

  Sensitive commercial information and intellectual property are attractive targets for data thieves. These include data about assets (geographical location, descriptions, and so on), operations and maintenance plans, inside knowledge about mergers and acquisitions, bid details, investment plans, trade secrets, and technological research. Attackers might also seek to acquire live data from sensors that monitor smart grids and even Wi-Fi networks connected through smart meters, which means that consumers can find themselves being both victims and, inadvertently, attackers.

  Attacks launched to capture corporate data are likely to involve several different techniques. An example is Operation Night Dragon, which was conducted through a series of progressive intrusions. Attackers compromised web servers, and then they accessed internal desktops and servers and obtained user authentication details to gain access to project-financing information linked to oil and gas field bids and operations.

  Successful attacks exploit human vulnerabilities and technical ones. Spearphishing and social engineering (using the techniques of persuasion to obtain confidential information) both played a part in the Night Dragon attacks. For details, see “Exxon, Shell, BP hacked in Night Dragon attacks,” ComputerWeekly.com, February 24, 2011:

  http://www.computerweekly.com/news/1280095257/Exxon-Shell-BP-hacked-in-Night-Dragon-attacks

Such attacks are likely to be carried out over long periods of time. Advanced persistent threats present one of the greatest dangers. An organization’s computer system can be infiltrated, and ongoing data theft can be active over a period of weeks or even months.

Consider what is required to execute a successful attack. The typical attack spans five steps that, together, form what is referred to as an *attack chain*:

1. Break in. This represents the initial entry, whether through a firewall, a web portal, or malware inside email.
2. Latch on. Now with access, attackers get their access privileges embedded into a system, deploy malware, set up back doors and communications with the organization, and escalate their privileges to those of an administrator.
3. Expand. The attackers move around in the network from system to system, infecting other systems as they go.
4. Gather. After the sought-after information is located, the attackers move that information to a location that is hidden so that it can be moved outside of the organization.
5. Exfiltrate. Finally, attackers transmit the stolen information to their home organization.

There are many variations of attack chains. But the point is that for an attack to be successful, it must progress through a series of steps to achieve an objective, whether the objective is to steal intellectual property or to destroy or disrupt uranium centrifuges.

The ability of the IT industry to protect itself is hampered by organizational weaknesses, notably low levels of security awareness and poor governance. These shortcomings are compounded by technological vulnerabilities, including existing hardware and the increasing use of the Internet as a means of control.

The sections that follow describe the concerns and difficulties.

Technological vulnerabilities

Many of the physical devices used in today's control systems, such as intelligent electronic devices and remote terminal units, were designed 20 years ago when isolation was presumed. These devices were never intended to be controlled over the Internet, and many lack basic security features. The lack of maturity in ICS and SCADA security domains provides a rich feeding ground for all sorts of attackers. Two vulnerable areas stand out in particular:

- Control centers are a soft target. Production Planning and Control (PPC) systems are widely used. External connectivity, including insecure remote access using dial-up connections, presents a significant risk.
  - Isolated systems are not immune from attack. *Bridged* networks are increasingly used to bring older equipment and control systems into the digital fold. Such systems are vulnerable to malware and proxy remote attacks.
  - Every endpoint is vulnerable. It is not only industrial control systems that are at risk but also the facilities, field equipment, and devices that are directly controlled by the systems.
  - Energy and utility enterprises are racing to adopt novel technologies, yet new automation and communications technologies expose businesses to new vulnerabilities unless they are carefully managed.
- Wireless technology represents a weak link. Radio frequency transceivers can be used to compromise sensors that monitor variables such as flow, temperature, and pressure. Attackers can trick control systems into shutting down processes simply by hacking sensors and generating fake readings.

Organizational weaknesses

One of the greatest areas of weakness across all industry sectors is a lack of security awareness. Organizations fail to identify threats because they are unable to identify what those threats are, where to look for them, or what to do if they turn into attacks. There are several other organizational weaknesses:

- Many organizations have failed to adapt. They are still using security models dating back a decade or more, and they lack the skills needed to secure the increasing mix of new and existing equipment for which they are responsible.
- *Box checking* is not a substitute for security. The industry remains over-reliant on rigid, compliance-based mechanisms that do not consider the complexity, constant evolution, and real-time nature of cyber threats. Governance is often poor. Many organizations have been slow to address the convergence of IT and operational technology (OT). Opportunities are being missed. For example, OT should be supporting enterprise governance, risk management, and compliance efforts. Currently, it rarely does.
- The IT industry struggles to get a big-picture view. An enterprise-only Security Operations Center (SOC), for example, is not enough. Companies need an industry-wide SOC perspective, because all critical infrastructure organizations inhabit a common threat landscape. Currently, management lacks the tools to build situational awareness, gather intelligence, and apply forensics.
- The supply chain is a major point of vulnerability. One of the biggest risks in the energy sector, for example, is access to enterprise or operational networks by third-party vendors. Energy and utility companies unwittingly reveal huge amounts of information about operations. Staff might blog, tweet, and update social network pages with project details. Even job vacancies can reveal too much, as when advertisements disclose which technologies are being used to provide security.

- Conventional IT security can no longer be relied on. Log-in IDs, passwords, and other forms of knowledge-based authentication are being undermined by the Internet. The explosion of social media means that personal details are now often publicly available.
- Organizations often cannot manage these risks alone. Identifying threats, protecting assets, and delivering business value require the assistance of an external partner with expertise and understanding of the critical infrastructure sector as a whole.

Let’s look at some examples of organizational weaknesses. In 2012, the term *watering hole* was introduced to describe attacks that target specific groups of users by injecting malicious code on the websites where such users congregate. Several new watering hole attacks occurred in 2014, such as an attack targeting readers of defense and military news websites.[9] In another case, researchers discovered malicious code on an industrial website that catered to automotive, aerospace, and manufacturing companies.[10]

Similarly, *malvertising* is an exploitation vector consisting of a compromised advertising network that serves malicious code that has been injected into ads displayed on legitimate sites. This allows attackers to reach a much larger audience than when compromising a single website. It also provides a way to target companies that might have tighter security around their own servers but, unknowingly, are serving malicious ads that are embedded in their content. In both watering hole and malvertising attacks, attackers are able to deploy exploitation kits to vulnerable endpoints by taking advantage of several browser-based vulnerabilities and by targeting plug-ins, such as Java and Adobe Flash.

In 2014, the vulnerability forecast shifted drastically when an automated tool identified a class of vulnerabilities affecting thousands of Android apps with improper SSL certificate validation.[11] These vulnerabilities allowed an attacker to perform man-in-the-middle attacks against affected mobile applications. Depending on the type of targeted application, the attacker was able to execute code or obtain sensitive information (personal, financial, or other information) to use to perform additional attacks. The *man in the middle* is there and has power, despite being invisible to the user. He can access more than personal data, because he can also gain control over a cell phone, for example, and the user probably will not notice what is happening nor how the phone is being spied on.

[9] “How can your organization better prepare for a security incident?” IBM X-Force® Threat Intelligence Quarterly, Q4 2015, Page 10.
http://www.ibm.com/security/xforce/downloads.html

[10] *Op. cit.*

[11] *IBM X-Force Threat Intelligence Quarterly*, 1Q 2015, Page 18.
http://www.draware.dk/fileadmin/IBM/X-Force/X-FORCE_Q120145Trend_Rapport__2_.pdf

Types of threats

Now, it is time to take a close look at some of the details behind relevant threat vectors. We begin by looking at the anatomy of an APT, depicted in Figure 3, and then we explain some of the details behind an opportunistic attack. For full details about this attack, see the Adobe Security Bulletin released August 12, 2014 about vulnerability identifier APSB14-19:

https://helpx.adobe.com/security/products/reader/apsb14-19.html

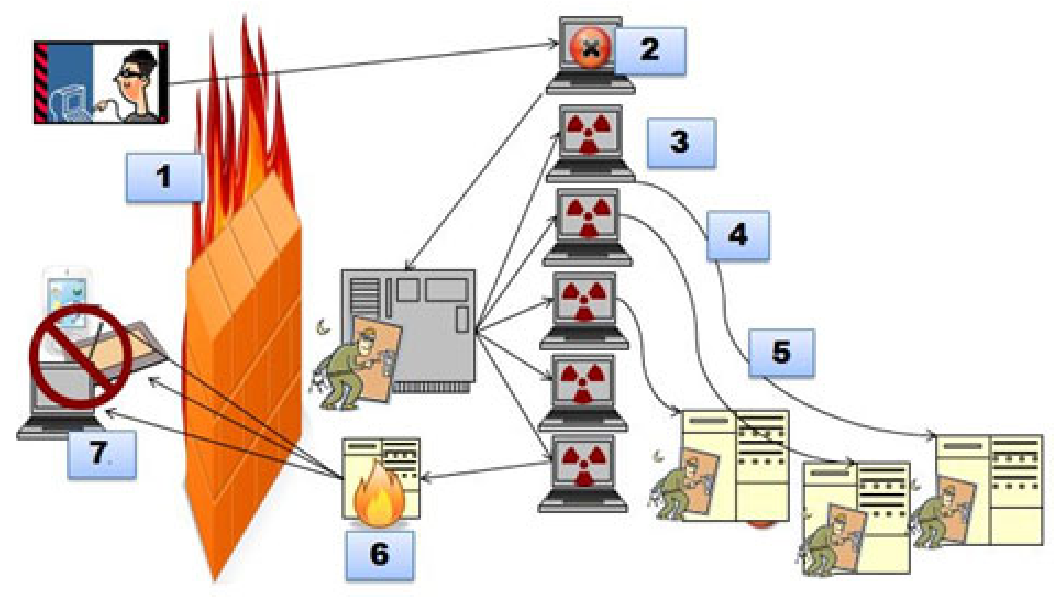


Figure 3 Anatomy of an APT

Next, let's examine this anatomy one step at a time, according to the numbered sections in Figure 3:

1. The attacker compromises a system administrator's device through a spearphishing attack. He takes advantage of a *zero-day*[12] vulnerability in the Adobe Acrobat Reader delivery mechanism with a crafted PDF. This is successful because the attacker assumes that the administrator regularly uses his device to read Adobe PDF files. This leads the administrator into the trap.
2. Then, the attacker uses compromised administrator credentials to access the Active Directory domains and to gain access to other systems through the *web of trust*.[13]
3. The attacker uploads other malicious code to more workstations by using his gained administrator access. Some of the malicious code might wait (persist) for the next campaign by the attacker.
4. Over time, the compromised workstations acquire additional login credentials for other servers in the network and spread the malware to them also. With this, the attacker can access those systems even if the initial device shuts down.
5. The attacker establishes back door access to multiple devices and creates secure, covert tunnels, possibly virtual private networks (VPNs), for data exfiltration.

[12] *Zero day* refers to a software threat that has a short amount of time to negatively affect systems or data. When the threat becomes known to the application developer, there are zero days to address the threat.

[13] A web of trust uses dual cryptographic algorithms for authentication.

6. The malware systematically targets certain data in a stealthy manner, yet, at the same time, destroys logs and evidence in an attempt to thwart forensics if detected at some point. The attacker does this for the initially compromised machine and also cleans up all compromised devices to eliminate any evidence that could possibly be left behind.
7. During this time, some level of data destruction or interruption might occur as a distraction technique to turn focus to that event versus the true target of the campaign.

Compare this approach to the attack chain of break in, latch on, expand, gather, and finally exfiltrate in the description of the *attack chain* (see “What attacks look like and how they work” on page 7.) The attacker in the attack chain moves through all of these steps. At every step, the attacker could have been stopped if the correct countermeasures were in place.

Another type of attack, shown in Figure 4, depicts the anatomy of an *opportunistic attack*. This type of attack is not a sophisticated one, but it is still effective.

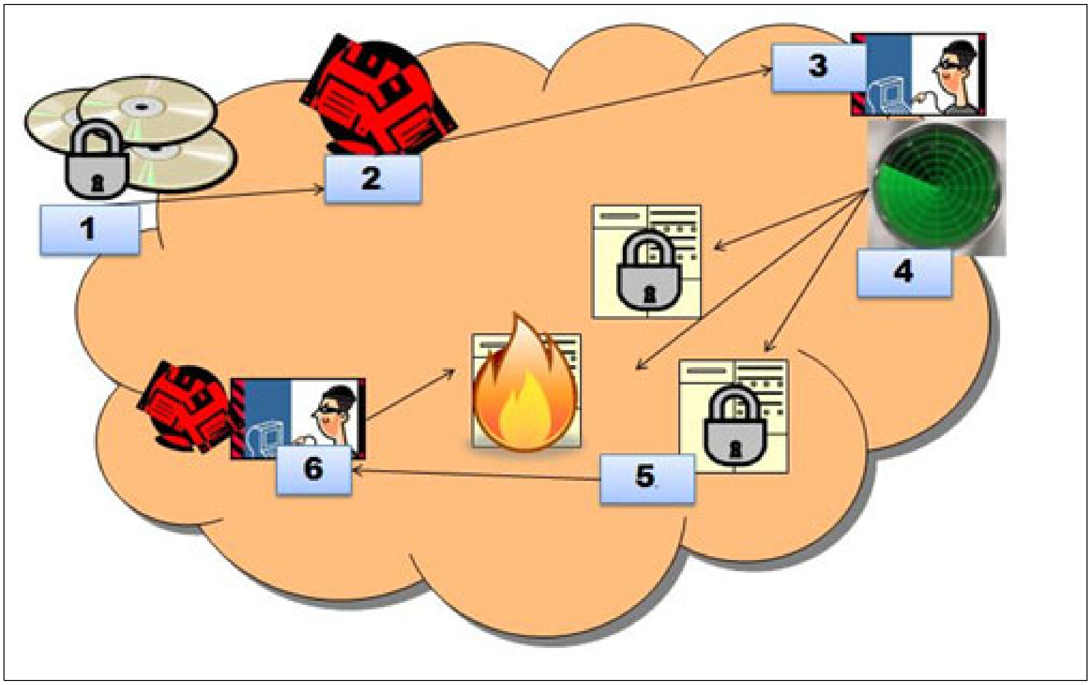


Figure 4 Anatomy of an opportunistic attack

Let us examine this anatomy one step at a time:

1. A security patch is released for a recently disclosed vulnerability in a web application. The release of this patch notifies the public that the vulnerability exists.
2. Attack kits, or malicious software offerings, are immediately designed to take advantage of the vulnerability on devices that do not receive the software security patch.
3. Attackers update their reconnaissance and scanning software to search the Internet for web-facing services that have not had the security patch applied.
4. Scanning software continuously takes note of each vulnerable device or service it discovers.
5. An unpatched web server is discovered by using the scanning software.
6. An attack is launched against the unpatched device, which then crashes or halts all of the services provided by the device. The device remains offline until it is repaired and patched.

What makes assets most vulnerable to attacks

As you can see, for an attack to be successful, it must move all the way through the attack chain. This gives the defender (you) several places where technology can be introduced to detect and help stop the attack. In fact, this demonstrates why technology alone has not been the problem. Usually, it is not the technology that fails but its deployment and overall integration.

This is not to say that every security gap or vulnerability has a technology to address it. What this means is that the use of security technologies or, more specifically, the inability to effectively use security technologies has been the problem. Therefore, it is important to understand that attackers are exploiting human behavior more than they are exploiting vulnerabilities in technology.

Technology vulnerabilities provide the means that attackers use to defeat some of the technical barriers in their path. Ultimately, it is the inability to recognize an attack and the ineffective responses that attackers are exploiting in a centrally correlated and timely fashion. This key insight is going to help us fight the attackers.

How we fight back

Imagine for a moment that you are a hacker. Given your knowledge of your industry, imagine being assigned a target from your government, military, or organization's leaders. You are given access to all of the computing resources that you need in addition to a team of specialists, such as engineers, industry security subject matter experts (SMEs), hackers, and so forth.

You and your team know the playbooks, the compliance requirements, the security frameworks, and the industry practices. You also know how people in your industry tend to operate and how their business processes, internal controls, and operational practices function. From this information and the experts you have been provided, you plan the attack.

What you will find is that the attack is much more about behavior and processes and reactions than technology. You know what people are looking at, what they tend to ignore, what they tend to react to, how they react, and how quickly. The reality is that the detection of sophisticated attacks is difficult, and responding to an attack in a fast and effective manner is even more difficult. How can you fight this?

The security mindset

The answer is that we need to change our security mindsets. We need to break away from existing and outdated security paradigms and adopt a new way of operating. The diagram in Figure 5 summarizes what that looks like.

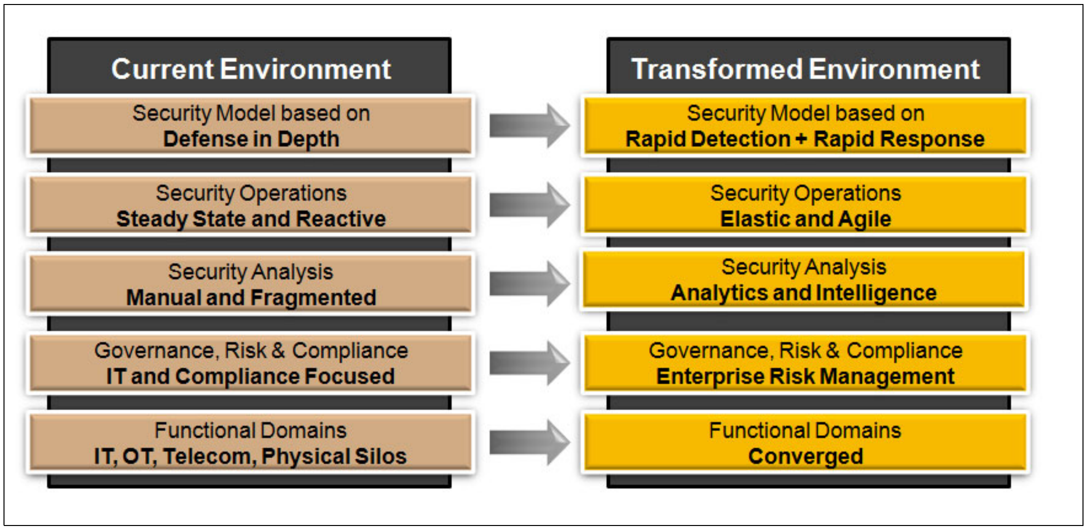

Current Environment
Transformed Environment
Security Model based on Defense in Depth
Security Model based on Rapid Detection + Rapid Response
Security Operations Steady State and Reactive
Security Operations Elastic and Agile
Security Analysis Manual and Fragmented
Security Analysis Analytics and Intelligence
Governance, Risk & Compliance IT and Compliance Focused
Governance, Risk & Compliance Enterprise Risk Management
Functional Domains IT, OT, Telecom, Physical Silos
Functional Domains Converged

Figure 5 Transforming the mindset about security paradigms

Security models based solely on the Defense in Depth[14] model are no longer effective against anything more than casual attackers. In general, this model is designed to detect and stop access and malicious activity from users with unauthorized credentials by building hardened perimeters and ring-fencing critical assets. That was effective in the 1990s and early 2000s. But today, most accomplished attackers are attaining authorized and privileged credentials early in the attack chain, making it easy to pass through traditional Defense in Depth controls.

Stuck in the Defense in Depth mindset, many organizations' IT teams' natural reactions to the increasing number of successful breaches has been (and still is) to build the walls higher and to add more layers, heavily segmenting their networks. This adds significant cost, complexity, and impact on the business and users. Imagine the frustration when the additional cost and effort does not slow the rising incident rates.

The change that is required is to break out of the Defense in Depth mindset toward *rapid detection and rapid response*. We need to design systems that are much more proactive at detecting suspicious or malicious activity, which is more about what is happening in the system at every point in time.

Security operations

The next major area that needs to change is security operations. Most organizations are still locked into fairly static and reactive operations, tied tightly to the traditional Defense in Depth model. This is to say that when alarms go off at the barriers, we react with incident response. But the change that we need to make is all about *visibility* and *control*.

Visibility relates to our internal and external situational awareness, which means monitoring what is happening inside our organization and relevant events outside of our organization. Monitoring is nothing new, but there simply has not been enough of it nor has the data been

[14] *Defense in Depth* is the use of multiple layers of authentication in a system to provide a greater depth of security.

used well enough to actually detect suspicious or malicious activity within our information systems. Many organizations are still struggling to effectively deploy security information and event management (SIEM) capabilities into their IT environments, so they have not yet extended SIEM into their OT (such as SCADA) environments, telecom, physical, and business applications.

We need to deploy sufficient technology throughout the attack chain to enable more visibility and control. We need to improve the way we respond, specifically how fast and focused the response is. One way to achieve this is by correlating early warning indicators, such as those from IBM X-Force Research and Development and CrowdStrike, and then correlate that with internal situational awareness. This can be achieved with a strong SIEM and security analytics solution.

Most important when there is a security event is the ability to address suspicious activities with agility and speed. Attackers can anticipate how long it is going to take an organization to respond and how they will do it. They will use that knowledge to their advantage. How long, for example, does it take your organization to execute an enterprise-wide password change? In many cases, this can take up to four months. Can you imagine what an attacker can do in that amount of time?

To increase agility in our responses, we must change how we operate. The goal is to establish predefined levels of security posture that an organization can respond to quickly.

Let's look at an example: Your SOC reports an early warning indicator, because several peers in the industry have been hit with a coordinated attack. The attack involves a zero day exploitation of a common firewall, a distributed denial-of-service (DDoS) attack to distract, and social engineering amid the confusion.

Receiving the warning, the chief information security officer (CISO) initiates a heightened state of awareness that the company calls Threat Condition Alpha, the initial (lowest) level of heightened awareness. Threat Condition Alpha is based on the integration of all of the system controls that can measure against business-based key risk indicators (KRIs). In other words, IT, risk, legal, and the lines of businesses have all agreed to and been involved in defining the different levels of threat conditions. With Threat Condition Alpha in effect, badge access into the building gets more restrictive, and a host of other measures are taken.

If the organization moves to Threat Condition Bravo, things become more serious. The SOC begins double work shifts to look deeper into the data. The intrusion prevention systems (IPS), intrusion detection system (IDS), and analytics thresholds are adjusted to log more suspicious events, delving deeper into the "noise." This was made possible by an earlier agreement with a local vendor that they would provide staff if such an event occurred.

If the situation becomes still more serious, Threat Condition Delta is activated. At this level, all remote access, including from mobile devices, is shut down. Only administrators can access the systems through jump boxes,[15] and logging and monitoring becomes focused on the administrators' exact movements and keystrokes. Buildings are restricted to key personnel only, using much more restrictive physical access lists. Video surveillance is increased and video analytics resources begin processing three times as much video in real time, and so the scenario continues.

These different levels of threat conditions are depicted in Figure 6. These are not static levels; they can be defined differently for each organization. It is important to have such a model defined in every operational plan. This is essential to eliminating guesswork during an actual incident.

[15] A jump box, or jump server, manages the security of multiple servers across secure zones.

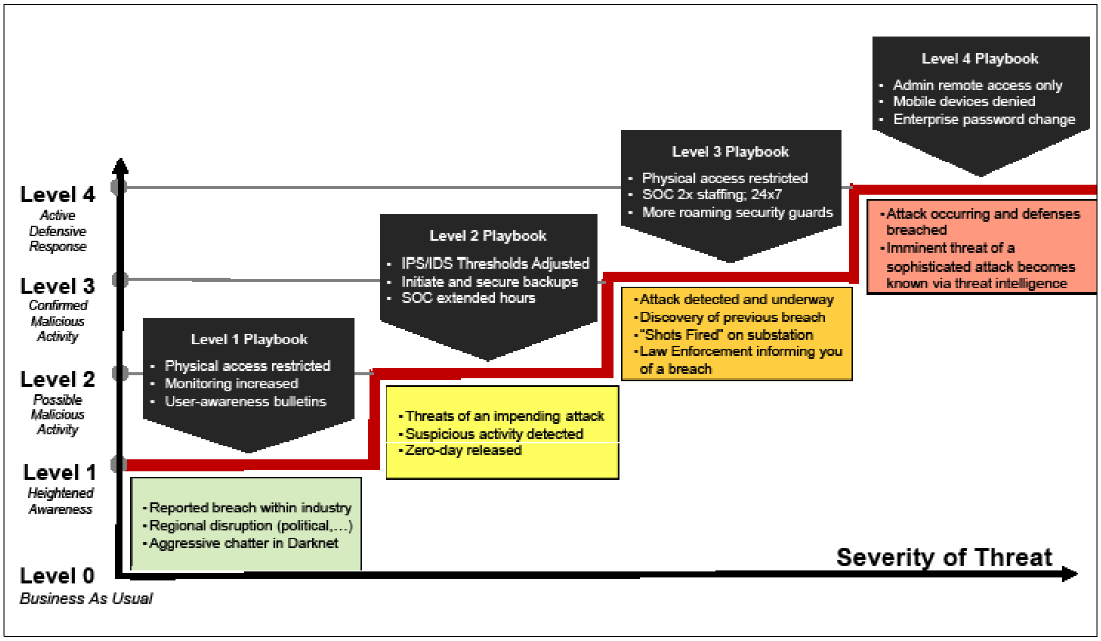

Level 4 Playbook
Admin remote access only
Mobile devices denied
Enterprise password change
Level 3 Playbook
Physical access restricted
SOC 2x staffing; 24x7
More roaming security guards
Level 2 Playbook
IPS/IDS Thresholds Adjusted
Initiate and secure backups
SOC extended hours
Level 1 Playbook
Physical access restricted
Monitoring increased
User-awareness bulletins
Level 4
Active Defensive Response
Level 3
Confirmed Malicious Activity
Level 2
Possible Malicious Activity
Level 1
Heightened Awareness
Level 0
Business As Usual
Attack occurring and defenses breached
Imminent threat of a sophisticated attack becomes known via threat intelligence
Attack detected and underway
Discovery of previous breach
"Shots Fired" on substation
Law Enforcement informing you of a breach
Threats of an impending attack
Suspicious activity detected
Zero-day released
Reported breach within industry
Regional disruption (political,…)
Aggressive chatter in Darknet
Severity of Threat

Figure 6 Levels of threat conditions

Getting security right requires a big-picture view

Key infrastructure security decisions are routinely delegated to individual divisions or departments (or even to third-party equipment suppliers) with limited security expertise and no overarching view of the threats now facing the industry. IT and OT still work in isolation, and most organizations lack the individuals who understand both environments, thereby increasing unnecessary risks.

With that in mind, the importance of predefined threat condition levels becomes clear. They can be activated nearly instantly. Because these threat level conditions have been predefined by the IT group in concert with groups from business and operations, the staff understands and accepts the impact of the threat conditions. Everyone in the organization understands what it means when a particular level is activated, and everyone understands their responsibilities. In this way, improved security roadmaps can be built.

For example, these methodfs can enable an organization to implement threat condition levels:

- To allow a strict physical access model with multiple levels of restrictions, an organization needs to deploy badge readers to all sensitive physical areas. These readers need to be centrally managed so that a change in access policy can become effective immediately. Levels of step-up authentication can be added by setting up optional biometric access systems (for example, fingerprint readers or iris scanners) for especially sensitive areas.
- To enable enterprise-wide password change enforcement in your organization, you need to deploy a centralized identity and access management solution. This enables the security administrators to enforce a mandatory password change when users log in to their systems. Be sure to eliminate any hardcoded administrative user IDs and passwords. Instead, deploy a privileged identity management system that can be tied to the central identity management system and, therefore, to the general password reset action.
- To immediately increase the level of centrally collected log and event data, you need to deploy a centralized security information and event management system and combine this with a powerful security intelligence solution.

This is the kind of elasticity and agility that enables an organization to counter today's and tomorrow's threats. This is the transformational change that you must achieve in your security organizations, including people, processes, and technology.

The changes that security systems have to go through are depicted in Figure 7.

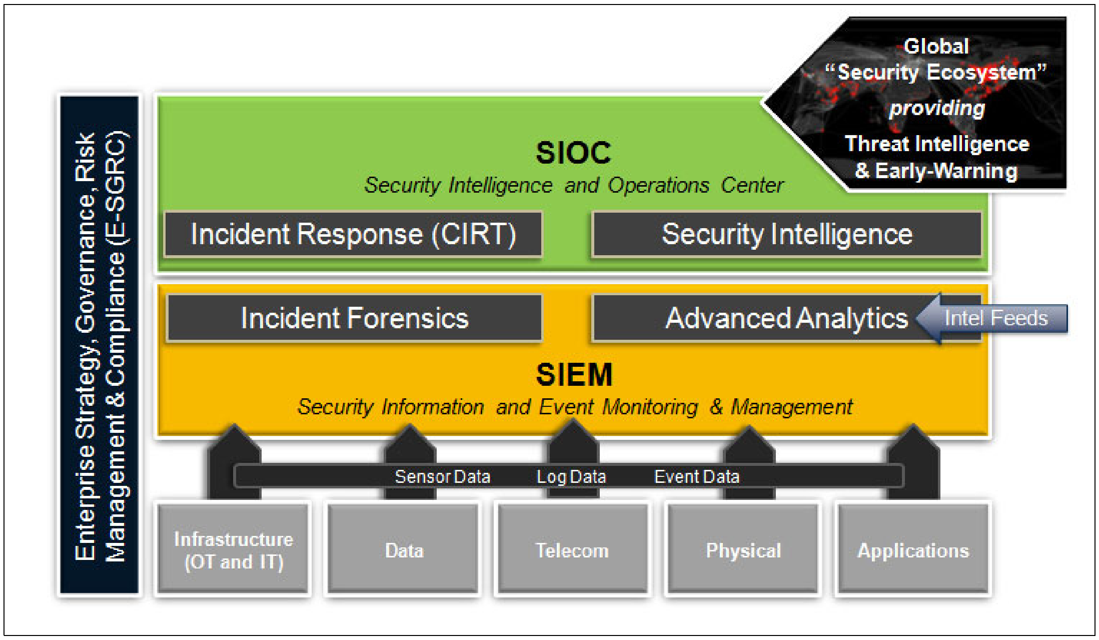


Figure 7 Realization of the new security approach

On its own, SIEM is not enough to protect your organization from harm. Proper offense correlation needs to use advanced analytics and security intelligence capabilities that can go beyond IT-centric investigations and include behavioral and social aspects.

For example, targeted phishing emails, a DDoS attack, and abnormal behavior of a database administrator who accesses client data are three events that might look unrelated. However, they can all belong to a well-organized and prepared attack.

This is where security intelligence comes in. For example, why check on a database administrator's data access when the administrator is trusted and follows security compliance? But then, why did the administrator look at so much client data within a certain period of time and afterward send an email with a large attachment to an external recipient? Maybe the DDoS attack was nothing but a distraction, during which time the phishing email gained the attacker access to the administrator's system and the attacker is now in possession of the data.

Security intelligence systems, such IBM QRadar® Security Intelligence Platform, can help protect you from an attack like this by distinguishing between normal and abnormal behavior. The system can tell what the database administrator usually does, and how the person or people in that role behave. The moment this behavior changes, it raises a red flag and reports that to the Security Intelligence and Operations Center (SIOC). As soon as SIOC personnel receive the incident report, they can raise the threat levels and initiate appropriate countermeasures.

But the job isn't done at this point. It is not only about detecting and stopping the attack; it is also about finding the source and capturing the attackers. Incident forensics support you with that. IBM QRadar Incident Forensics, for instance, helps an organization investigate the events after they have occurred and then gather evidence against the attacker.

The following actions are essential to implement this new security approach:

- Monitoring

  Monitoring is the basis of intrusion detection and prevention. The sooner you realize an abnormality in your system, the faster you can respond. IBM monitors more than 15 billion security events every day, from nearly 4,000 security clients in 133 countries, using a database of more than 81,000 security vulnerabilities.

- Research

  Be up to date. Know what the current threats are and what the threat impact is. The IBM X-Force Research and Development team researches and evaluates vulnerabilities to help keep your organization secure.

- Education

  The better your employees understand what's going on and how real the threat is to them, the more they will participate and play their parts in this fight. To successfully protect your organization, all involved people must be educated.

- Integration

  Do not keep security separate from your business. Integrating security into your business and operations gives you the opportunity to react fast and effectively.

- Exchange

  Learn from others. Share your experiences across your organization and with trusted partners in your industry sector around the globe. The bigger the exchange, the smaller the chances for attackers. IBM X-Force Exchange provides you with an open source intelligence platform built on more than 700 TB of cybersecurity data.

That is what IBM brings to the market: Providing elasticity and agility to enable rapid detection and rapid response. We can help you with an assessment to determine where you are today in terms of security, including strengths and weaknesses, and review your most valuable assets and processes. Together, we will plan how you can get to where you need to be. We can enable you to prevent attacks in real time, to detect malicious incidents by using security intelligence, and to defend against web fraud and cyber crime.

Business case

Now that you have learned about how to fight back and how that knowledge can be applied in the real world, let's review a business case.

Business environment

The client is a multibillion-dollar energy utility firm. The organization operates globally and plans on becoming active in more countries in the near future. The company has several contracts with governments. To achieve a competitive advantage, they have acquired several companies. This has led to fairly autonomous business units, each with its own business culture. Including all, the current number of employees is about 100,000.

Because of the strategic nature of the client's products and processes, the infrastructure is considered critical. On the plant floor, for example, the business is highly automated and uses extensive industrial control systems.

This client invests greatly in renewable energies and recently acquired a startup company with innovative ideas. Therefore, the protection of intellectual property is important to the organization. Civil commotions in some countries add the risk of a politically motivated attack. The competitive pressure of the industry, which could also lead to attacks, cannot be ignored.

The client had been hit with hacktivism in the past. Fortunately, no harm was done, but the managers realize that their way of handling security must change.

Current security landscape

The client relies heavily on static IT perimeters and defenses, such as firewalls and an IPS. They have not implemented a centralized SIOC yet and are just beginning to deploy a SIEM.

At this time, security is not well integrated and is disconnected from the operations team. Although a few people are assigned to address security issues, they are heavily involved with daily operations and cannot pay as much attention to security as needed. Therefore, the client counts on ad hoc incident response but has no IR plan. A strategic partner does not exist; however, depending on the geography, various local small players are engaged.

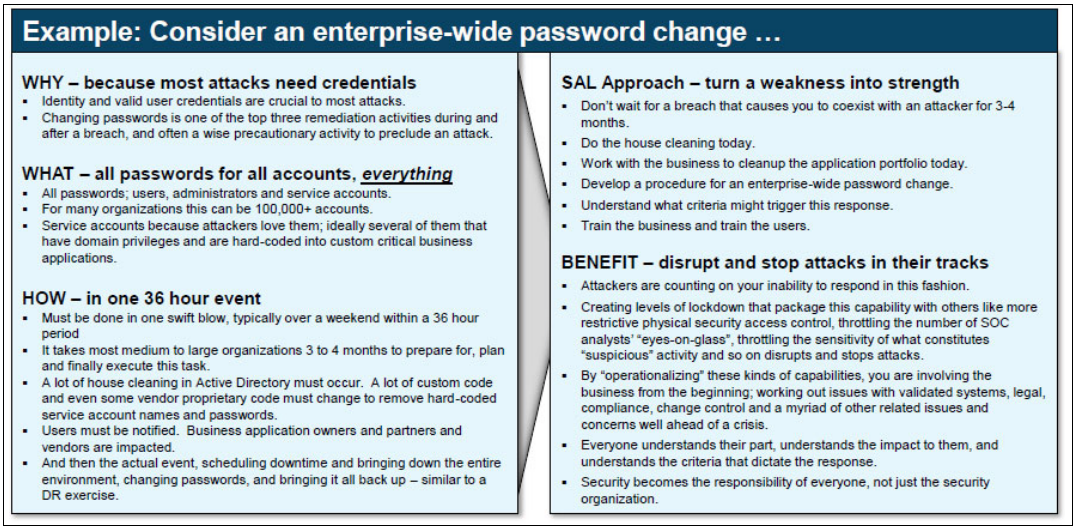
Because of the changing threat landscape and the awareness of the risks that the client is facing, they want to mature and transform but are unsure where to begin. After the hacktivist attack, the board is demanding quick results, but the security budget is limited (1 - 2% of IT expenses). Additionally, only a small increase in head count is approved, and the organization's culture is rather resistant to security controls.

Security transformation

The tasks that IBM representatives face are to develop an incremental plan, beginning with a focus on operations, and to determine where the most impact can be achieved with the least amount of up-front spending.

To fulfill these requirements, the IBM team starts by taking an inventory of existing technologies and then evaluates how the team can optimize them to properly respond to events in the attack chain.

As a starting point, the IBM team deploys one new technology (a centralized identity management system) to enable rapid password changes, as depicted in Figure 8.



Example: Consider an enterprise-wide password change …

WHY – because most attacks need credentials

- Identity and valid user credentials are crucial to most attacks.
- Changing passwords is one of the top three remediation activities during and after a breach, and often a wise precautionary activity to preclude an attack.

WHAT – all passwords for all accounts, *everything*

- All passwords; users, administrators and service accounts.
- For many organizations this can be 100,000+ accounts.
- Service accounts because attackers love them; ideally several of them that have domain privileges and are hard-coded into custom critical business applications.

HOW – in one 36 hour event

- Must be done in one swift blow, typically over a weekend within a 36 hour period
- It takes most medium to large organizations 3 to 4 months to prepare for, plan and finally execute this task.
- A lot of house cleaning in Active Directory must occur. A lot of custom code and even some vendor proprietary code must change to remove hard-coded service account names and passwords.
- Users must be notified. Business application owners and partners and vendors are impacted.
- And then the actual event, scheduling downtime and bringing down the entire environment, changing passwords, and bringing it all back up – similar to a DR exercise.

SAL Approach – turn a weakness into strength

- Don't wait for a breach that causes you to coexist with an attacker for 3-4 months.
- Do the house cleaning today.
- Work with the business to cleanup the application portfolio today.
- Develop a procedure for an enterprise-wide password change.
- Understand what criteria might trigger this response.
- Train the business and train the users.

BENEFIT – disrupt and stop attacks in their tracks

- Attackers are counting on your inability to respond in this fashion.
- Creating levels of lockdown that package this capability with others like more restrictive physical security access control, throttling the number of SOC analysts' "eyes-on-glass", throttling the sensitivity of what constitutes "suspicious" activity and so on disrupts and stops attacks.
- By "operationalizing" these kinds of capabilities, you are involving the business from the beginning; working out issues with validated systems, legal, compliance, change control and a myriad of other related issues and concerns well ahead of a crisis.
- Everyone understands their part, understands the impact to them, and understands the criteria that dictate the response.
- Security becomes the responsibility of everyone, not just the security organization.

Figure 8 Benefits of a centralized identity management system

In addition, the team invests in external security intelligence and early warning providers. With the long-term plan to outsource the SIOC operations, the IBM team uses the Network Operations Center (NOC) in the short-term. The security team deploys more SIEM logging capabilities and extends those into operational environments and protocols. They also begin to make better use of analytics and automation in the SIEM area for correlation and behavioral analysis to improve attack detection and response. That way, the client can respond faster, plus more efficiently and with more assurance.

For incident response, the team selects a global strategic partner and co-develops an incident response plan. On top of that, the goal is a managed device administration with long-term transitions to Managed Security Services (MSS).

For all of this to work as planned, it is essential that all involved parties, including the employees, are onboard. Therefore, the IBM team initializes culture change management by using governance restructuring, training, and a communication program. Where possible, the team retools and cross-trains staff. They outsource other tasks. This is important, because making sure that everyone understands the risks and what they can do to avoid them ensures a much higher participation in the realization.

Additional results

This project more than met the client's needs. A post-deployment analysis identified several additional benefits of this approach:

- Executive showed more confidence in the ability to defend against attacks.
- The results were highly visible to the board of directors and the employees.
- Security training became more relevant and was taken more seriously.
- Integration between incident response, disaster recovery, safety, and other response plans became tighter, and a greater clarification of security governance and responsibilities was achieved.

Summary

To summarize our findings about industrial security controls, we want to make three important points:

- Intelligence is the new defense.
- Integration is the new foundation.
- Expertise is the new focus.

The way that security is enabled must change. Elasticity and agility must be improved so we do not give hackers opportunities. Those who attempt to hack and harm businesses never stand still, and they are connected. As they become more and more sophisticated, we must do the same. We have to move faster in detecting, preventing, and responding to attacks. We cannot afford to give attackers time to navigate our systems or steal or destroy data.

It is no longer about technology. Security today is mainly about behavior. Most attackers perfectly understand our behavior, and they use it to their advantage. We can do the same.

Let's educate our staff to make them sensitive to social engineering. Let's integrate security in our daily business so we can stop these attacks.

Authors

This guide was produced by a team of specialists from around the world working for the International Technical Support Organization (ITSO).

James Eaton is a member of IBM's Critical Infrastructure Security Services team. He has provided security consulting services to corporations and public entities in the following industries: Oil and gas producers and distributors, utilities (hydro and nuclear), manufacturing, insurance, financial services, and healthcare. James has worked in municipal, state, provincial, and federal governmental organizations in North America and abroad. With more than 16 years of experience providing security advisory services to corporate leaders and management, James has developed, implemented, and managed enterprise security programs for medium-sized to large organizations in the private and public sectors in Canada and the USA while working for TELUS, Accenture, Entrust, Ritchie Bros., ICBC, and Chevron Corporation.

Craig Heilmann is an Associate Partner within IBM's Integrated Security division and practice leader for Critical Infrastructure Security Services. His career spans 20 years of technical, professional, managerial, and entrepreneurial experience applied in information security, controls, and governance. Before IBM, Craig was a United States Air Force commissioned officer specializing in intelligence and information warfare, founder of two high-tech security companies, and 10 years as an executive consultant for a large global services and integration company. Craig is an inventor included in 11 US patents, and a computer engineer and information security expert with MSEE, CISSP, and CRISC designations. His functional expertise and core competencies include industrial control systems security, enterprise risk and compliance management, security infrastructure and operations, incident response and remediation, telephony and merged (PSTN, VOIP, SIP) infrastructure security, and business process controls (SAP specialization).

Anja Jessica Paessler worked two years for technical magazines, mainly focused on automation. She joined IBM Germany in 2013 to take part in IBM University Programs in Ehningen. As part of the program, Anja has worked in IBM PureSystems® sales, Human Capital Management consulting, Social Business and IBM Redbooks® publications. In addition to being an IBM employee, she is a student at Cooperative State University Stuttgart, where she is studying International Management for Business and Information Technology and will receive her bachelor of science degree in 2016. She then plans to join the IBM Security bustiness unit.

Simone Riccetti is a Senior Security Consultant with IBM Professional Security Services. He is based in Italy but performs services in the Europe, Middle East, and Africa (EMEA) region. Simone focuses mainly on Cyber Security, maintaining both customer-facing relations and technical skills. Before working for IBM, Simone developed good skills through several international network and security projects, including design, implementation, and project management. His main interests tare in security testing, critical infrastructure, supervisory control and data acquisition (SCADA) security, application security, and big data, and analytics for intrusion detection. Simone has also worked as contract professor at University of Insubria (Como, Italy) and is collaborating with various universities in security research. He is a member of the European Union Agency for Network and Information Security Smart Infrastructures Security Experts Community (ENISA SISEC) group, which focuses on smart infrastructures security. He holds several professional certifications, including Certified SCADA Security Architect (CSSA), Certified Information Systems Security Professional (CISSP), Certified Application Source Code Security Analysis (CSSLP), Payment Card Industry Qualified Security Assessor (QSA), and PRINCE2 Project Management.

Rick Robinson is the Offering Manager for Encryption and Key Management for the Data Protection group of IBM Security. He writes often about security intelligence and frequently presents at IBM conferences on the topics of encryption, key management, PKI, certificate asset management, and hybrid cloud data protection.

Thanks to the following people for their contributions to this project:

Vasfi Gucer, Axel Buecker, Karen Lawrence, and Judith Broadhurst
IBM US

Now you can become a published author, too

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time. Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online:

ibm.com/redbooks/residencies.html

Stay connected to IBM Redbooks

- Find us on Facebook:

  http://www.facebook.com/IBMRedbooks

- Follow us on Twitter:

  http://twitter.com/ibmredbooks

- Look for us on LinkedIn:

  http://www.linkedin.com/groups?home=&gid=2130806

- Explore new IBM Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

  https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm

- Stay current on recent Redbooks publications with RSS Feeds:

  http://www.redbooks.ibm.com/rss.html

REDP-5323-00

ISBN 0738454915

Printed in U.S.A.