POSITIVE TECHNOLOGIES

CONVERGE IT & CRITICAL INFRASTRUCTURE PROTECTION

Issue 1

Featuring research from Gartner

Address these 8 network security pain points

It's no secret why malicious attacks on organizations large and small are on the rise: cybercriminals keep getting better at what they do.

By way of analogy, cybercriminals are like burglars looking for a way into a building: an open window or an unlocked door will do, but even something never intended as an entrance, like a ventilation duct, could offer a way inside.

Some bad guys employ automated bots that prowl networks, ceaselessly searching for vulnerabilities to exploit. Others reapply proven methods of attack on new victims. Perhaps you've read about breaches achieved through weak passwords or poorly protected minor systems that share segments with critical infrastructure. No matter what the method, a common thread in most attacks is exploiting software vulnerabilities and misconfigured system settings.

Well-prepared organizations are assessing and managing network vulnerabilities to lock down unintended entryways. They're constantly searching for anomalous activities that may be the sign of a multi-channel attack. They're developing rapid response plans to combat emerging threats including zero-day threats. They're integrating network security proactively across the enterprise to keep the bad guys out.

When organizations manage their vulnerabilities well, bad guys search for other companies that are easier targets. ***So stop being an easy target!*** If your organization still employs a fragmented approach to vulnerability management, you're in the path of least resistance. You're next.

What should you do? Manage your vulnerabilities. Gartner defines vulnerability management (VM) as "the key process for finding and remediating security weaknesses before they are exploited." Every other security measure, including, firewalls,

passwords and antivirus programs, builds on VM's foundation of continual assessment and remediation.

If you are responsible in some capacity for the security of critical business information and infrastructure networks, there are important questions you should be asking. Below are eight key VM "pain points" facing information security managers and professionals, and ways you can begin to address them through a foundational, integrated approach to vulnerability management.

1. "What can I do to keep our network secure?"

Broadly speaking, you must proactively identify vulnerabilities and potential attack vectors, assess and prioritize threats, and remediate weaknesses. But doing this across only a few systems will not keep you safe. You need to conduct black box and white box testing and security configuration assessments of all systems across the enterprise, including network, VoIP and wireless, OS, DB, Apps, ERP, Banking, Telco and SCADA. This process must be ongoing and include assessments of system security configurations.

2. "How can I stay ahead of the latest threats in a dynamic threatscape?"

Establish frequent, regularly scheduled, automated security assessments. Conduct real-time, ongoing scans to identify known threats and monitor for anomalous activity to sniff out emerging threats and unknowns. These steps can help minimize the time between discovery of a vulnerability and release of a malicious exploit. You will need access to a comprehensive and continuously updated knowledge base of security configuration parameters, benchmarks and vulnerabilities backed by experts on enterprise network security.

3. "How can I account for all of our networked assets?"

You can account for assets via network scans, but the important issue is how secure are all of these systems and applications against attack? You need to know the level of risk across your entire network, including network and telephony equipment, WiFi, databases, operating systems, and Web and mobile applications. And since your network constantly changes, it is vital to incorporate change management to provide ongoing visibility of your real-time security state.

4. "How can I ensure both my internally developed and off-the-shelf systems are protected?"

For systems under development, application security testing can help to ensure that systems are secure by design. Such tests can be crucial in addressing vulnerabilities in the growing number of Web applications and others developed in-house, many of which are designed to emphasize functionality, not security.

For systems in operation, both vulnerability scans and penetration tests can help to assess weaknesses in your production environment. Vulnerability scans are automated, inexpensive and quick ways to understand what known vulnerabilities exist that may be exploited. Penetration tests, on the other hand, safely exploit weaknesses due to normal business logic or that emerge through conflicts with new systems or applications, in order to evaluate your ability to protect your systems from attack.

Both types of assessments are critical parts of a comprehensive and active network security strategy.

5. "How do I know whether vulnerabilities and misconfigurations in one place affect another?"

You don't know – unless you reassess security every time you make a change. If you deploy patches to your systems, you need to rerun your assessment to see what has changed from the perspective of your security posture. You may have closed the vulnerabilities that you identified, but did you create any new ones in the process? An integrated approach is especially important to thwart cybercriminals using multichannel attacks to penetrate networks "protected" by fragmented VM.

6. "How do I translate vague compliance guidelines into operational security controls?"

Compliance guidelines usually describe desired outcomes, but since every organization is different they may not describe what you need to check and address in your specific network. For example, your business may have to implement and validate technical policies and processes that ensure secure data transmission, limit access or protect the integrity of customer or employee information.

[1]Vulnerability Management Practices and Vulnerability Assessment Technology, Anton Chuvakin and Eric Maiwald, Gartner, Inc. G0022698720, March 2012, page 5

A foundational, integrated approach to VM includes actionable, verifiable operational security controls. The more controls that can be analyzed, the quicker and easier it will be to validate the desired outcomes, and provide monitoring and continuous assessment to help prove ongoing compliance.

7. "How can I improve security workflow?"

Your security resources are likely constrained already, so it's important to identify and remediate vulnerabilities efficiently and before they can be exploited. If you automate scheduled security assessments, this can happen routinely. And by accurately pinpointing weaknesses, you can minimize the resources required to chase false positives and, more importantly, limit the number of false negatives which can put you at risk and give you a false sense of security.

8. "How do I know if what we are doing is working, and how do I demonstrate that to management?"

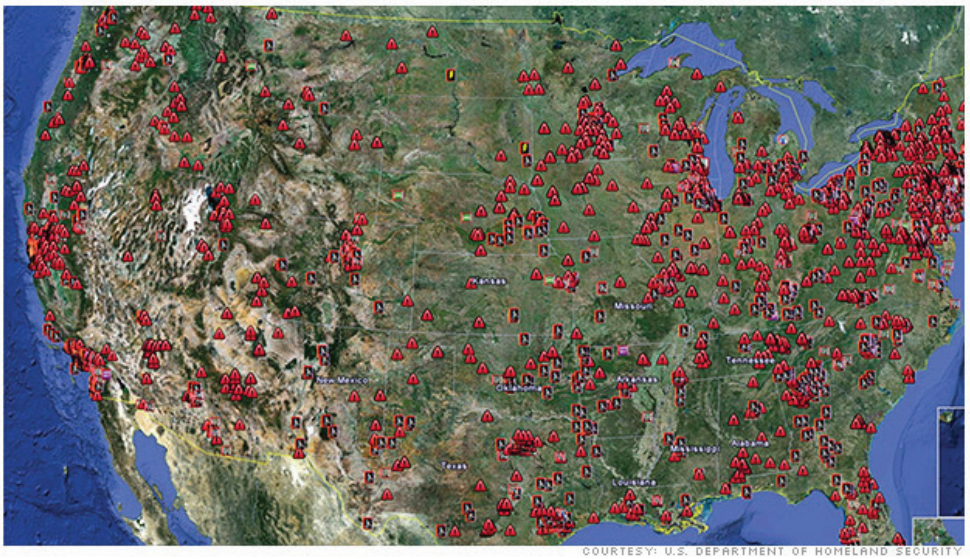
As with any measurement exercise, you need to establish baselines to quantify future performance. Define security KPIs in terms of the real-world effectiveness of your policies in protecting your business from unauthorized malicious intrusion and select a VM solution that provides you the historical data for reporting to various levels of the management chain or adapting your processes if necessary.

There's More At Risk Than IT

While "network security" equates to "IT security" to some information security people, integrated vulnerability management emphasizes a foundation of security across the entire enterprise. Businesses requiring high-level security and operating in tightly-regulated sectors, such as banking, telecommunications and utilities, are generally taking necessary steps to keep their IT networks secure, but vulnerabilities can exist in other places.

One potentially huge point of risk is an organization's operational technology (OT). These core systems encompass critical infrastructure that protects people and assets, monitors and controls physical devices, or changes the physical state of environments. This infrastructure is an increasingly popular target for attack by malicious agents, not only for the potential havoc a breach can create, but also because these systems often lack robust security.

Why? Because OT security is overlooked by organizations that view these systems as internal and cut off from the outside. However, security experts have clearly demonstrated that this is a mistake. Sophisticated cybercriminals understand that OT systems have not always been developed with security in mind, and crucial assets – or even entire networks – may be vulnerable. OT security today is at the level where IT security was ten years ago, and the bad guys know that they can find ways to access OT systems from the wild.



Approx. 7,200 key industrial control systems appear to be directly linked to the Internet

By example, supervisory control and data acquisition (SCADA) systems are widely-used in the energy sector to automatically sense, monitor and control physical processes such as those used to produce electricity, refine oil and regulate the flow of natural gas. Historically, SCADA systems were highly customized and proprietary, which made them difficult to attack without specialized inside knowledge.

More recently, however, energy companies and their control systems vendors have begun incorporating open standards technologies such as Ethernet and TCP/IP across their SCADA environments. While these advancements help improve services, productivity and profitability, they also dramatically increase the risk of critical services falling victim to cyber-attack.

Unless an organization is actively finding and fixing such vulnerabilities in OT systems and managing the remediation process, the risk from malicious intrusion is potentially catastrophic. Yes, catastrophic:

- An attack on an intermodal transportation system could bring a large city to a screeching halt.
- An attack on a power distribution network could darken a region and destabilize the grid.
- An attack on a nuclear plant could threaten the safety of millions.

Those are hypotheticals, but are they far-fetched? Consider this:

In July 2010, the Stuxnet worm validated long-held fears that sophisticated cyber-attackers could not only steal sensitive data, they could use that data to remotely sabotage physical processes in critical infrastructure environments. Since then, there have been several reported attacks on critical infrastructures like Shamoon knocking out 30,000 computers at oil and gas producer Saudi Aramco, the breach at Canadian energy giant Telvent and Red October; the largest cyber espionage incident on record.

What Can You Do?

Forward-thinking organizations have already started to walk away from the idea of viewing information security as a line item in the budget. They're rethinking their whole approach by investing in the process of vulnerability management. They're recognizing that IT and OT face complementary security risks that cannot be effectively protected in isolation. Rather, they must be viewed together and be made part of a unified enterprise security strategy.

Organizations evaluating potential providers of network security should look for a specialist resource that can identify vulnerabilities, prioritize remediation, align solutions with broader risk management goals, and never stop identifying vulnerabilities. Many network security vendors provide firewalls and antivirus software, but few truly understand foundational vulnerability management. It takes a great deal of highly specialized knowledge about the current state, ongoing research into a constantly changing threatscape, and insight to apply security intelligence effectively on an ongoing basis. It takes hands-on knowledge gained on real-world systems where people and organizations lie in the balance.

No matter the attack vector, cybercriminals operate on the premise that vulnerabilities exist. But you can lock the doors and windows. You can close ways in that were never intended to be ways in. You can remove the opportunity for bad guys to penetrate weak defenses.

Be Proactive—Get Started on Your OT Security Today:

+ Inventory all OT systems and equipment
+ Conduct Security Audit (passive and = active scans)
+ Perform deep technical inspection of OT security at Network/OS/Database and Application levels
+ Develop clear, proactive security policies
+ Define security configuration flaws
+ Develop hardening guides
+ Perform specific OT vulnerability research for:
  - 0-day vulnerabilities in core components
  - DoS attacks
  - Brute Force
  - Software and firmware vulnerabilities

Source: Positive Technologies

From the Gartner Files:

CIO Involvement in Operational Technology Vendor Risk Management Mitigates Security Vulnerabilities

Accountability for risk management of operational technology vendors is often unclear, but IT components imbedded in OT can potentially disrupt critical production processes. CIOs must get involved to help mitigate the immature software life cycles and security management processes of OT vendors.

Impacts

- OT vendors lack experience in addressing software life cycle and security management processes, and consequently introduce vulnerabilities to enterprises — CIOs are uniquely positioned to help manage these vendor risks across the entire IT/OT spectrum.
- Issues around authority, organizational boundaries and lack of trust between CIOs and operations/engineering team leaders prevent enterprises from adopting standardized vendor risk management practices across the IT and OT vendor ecosystem.
- Due to a lack of sharing, transparency and accountability among CIOs and operations/engineering team leaders, many common OT vulnerabilities are unknown to the enterprise and remain unmonitored — and could have potentially devastating consequences.
- Many OT vendor risk management programs are either nonexistent or too immature to enable CIOs to adequately and effectively mitigate enterprise-class vendor risks.

Recommendations

- Spearhead IT/OT executive steering committees and implement vendor risk management task forces, assigning liaisons to each affected line of business (LOB).
- Get directly involved in (but not take over) vendor risk management activities and raise awareness of OT vendor risks among LOB leaders.
- Sponsor, prioritize and ensure vendor risk management disciplines are adequately funded to increase maturity levels and effectively mitigate enterprise vendor risks.
- Standardize vendor risk management programs as ongoing disciplines across the IT/OT spectrum — providing risk assessment, contracting strategies, monitoring and mitigation efforts.

Strategic Planning Assumptions

By 2017, CIOs will develop vendor relationship skills as a top 5 competency, to extract business value and innovation from strategic vendors.

Until at least 2016, more than 70% of enterprises with significant investment in plant and production equipment will discover the need to take urgent action over the risks of serious operational and strategic failure caused by ineffective management of software-related OT issues or ineffective response to IT/OT convergence. In this context, "urgent" means that the risks are so serious that, once discovered, the enterprise will have to act to eliminate or reduce them within two months or sooner.

Analysis

Since operational technology (OT) is taking on more IT-like characteristics — and IT/OT convergence is creating new business opportunities — CIOs are being tasked with managing the digital business aspects of OT. However, due to the nature of their technology and objectives, OT vendors have placed far greater emphasis on automation improvements and performance than on risk management of their solutions and services.1 Because OT vendors have traditionally been sourced and managed through the LOBs, risk management of these vendors may have been solely focused on supply chain production, while security and software-related risk management has often remained unassigned or obfuscated.

Additionally, master product and services agreements have not been the historical norm for OT vendors, which have traditionally relied upon embedded license agreements. Therefore, negotiating T&Cs that are as protective as those found in IT vendor contracts can be difficult. As a result of these nuances, standardizing

vendor management activities — particularly vendor risk management practices — across the entire IT/OT continuum has become critical.

These challenges were introduced in the previous research document "Growth of IT/OT Convergence Creates Risks of Enterprise Failure." Here we explore these challenges in more detail and offer specific actionable advice.

When Should a CIO Consider Getting Involved in Managing OT Vendor Risk?

As stated in "2014 Planning Guide for Security and Risk Management:"

"The digitalization of business is accelerating, and in many cases the line separating IT and OT has started to blur. Many OT solutions now include components sourced from general-purpose IT vendors, such as hardware and software used in management systems. In addition, once physically separated IT and OT networks are often connected through bridging or gateway components. OT systems are therefore increasingly vulnerable to exploitation."

Furthermore, unlike many IT systems, OT systems are not designed to prevent the vulnerabilities mentioned above.

Security and software-related risk elements of OT vendors are often unidentified. This risk is compounded by OT vendors with too few best practices in place to assist in this type of risk mitigation. (Priorities for both the vendors and their OT clients tend to be focused on other elements of functionality.) Additionally, OT vendors typically do not have practices in place for the types of third-party certifications and audits that IT vendors have — such as SOC 2 and ISO 27001. (For more details on these standards see "SAS 70 Is Gone, So What Are the Alternatives?")

CIOs responsible for IT/OT converged technologies cannot rely upon the vendors to mitigate software-related risks. Instances of enterprise failures — and data loss resulting from OT-software-related intrusions — will continue to rise until CIOs take the lead in developing vendor risk management programs that encompass both IT and OT technologies. These risks are real and have already had adverse effects on many organizations. Although intrusion is only one of many types of OT risk, it has high visibility and is a good example that can drive home the message to stakeholders that OT vendor risk management must be addressed.

Key Intrusion Examples

Stuxnet

Stuxnet malware is an example of a successfully targeted exploitation of supervisory control and data acquisition (SCADA) systems and process control systems (PCSs). Stuxnet used multiple techniques to exploit vulnerable Windows PCs and servers, and from there found and compromised specific Siemens SCADA systems commonly used in power plants and other industrial operations. Although the Stuxnet malware itself was complex in nature, avoiding or mitigating most of the individual software flaws Stuxnet exploited was relatively simple. Stuxnet took advantage of weaknesses in security processes, which could have been avoided by the designers and customers if they had had a disciplined approach to vulnerability management.

Prof Password Theft

In this situation, a hacker using the handle "prof" was able to bypass security at water systems utilities. It is suspected that the hacker stole passwords housed in the OT vendor's systems. Through remote access to — and direct compromise with — SCADA systems, the hacker caused damage to equipment, causing burnout of at least one water pump. This type of hacking can occur when vendors are permitted to retain client password information without effective security being in place to protect their privacy.

Target Credit Card Exposure

In 2013, this highly visible failure hit retailers during their worst possible moment at the height of the holiday shopping season. Over 40 million customers may have been affected. The causes for the breach continue to be reviewed and analyzed. However, it is widely believed that the failure occurred with endpoint devices, through retail cash registers as "point-of-sale-malware," and not from network security failures. Although point-of-sale devices are not typical OT devices, this stresses the fact that endpoint, wireless or other devices that are not connected to the network can expose enterprises to risk (see Note 1).

CIOs are uniquely positioned to address an enterprisewide view of security and risk management/

mitigation. Also, they have the expertise among their IT personnel to execute effective vendor risk management programs through their security and vendor management teams. This research document explores the impacts of IT/OT risks and suggests specific recommendations for CIOs to address them.

CIOs should get involved in OT vendor risk management when:

- OT products are connected to the IT infrastructure.
- OT solutions contain standardized IT software and thus behave more like IT products.
- OT service providers have access to enterprise systems.
- IT service providers have access to OT-related systems.

When OT software is involved with critical business functions, outages or downtime concerns must be escalated through processes involving the OT vendor. These issues should also be tracked internally until they are resolved. Typically, IT departments already have trouble-ticketing processes in place for IT software that could be leveraged for the purposes of OT software issue escalation and tracking.

If there is a natural fit and benefit — and/or the CIO is responsible for IT/OT oversight — OT vendor risk management should be an integral part of the CIO's strategy. However, CIO involvement may not be necessary in all situations. If their contribution is restricted — whether through politics or capability/resource limitations — the OT vendor risk elements should still be monitored but handled elsewhere by a COO, director of quality assurance, chief risk officer (CRO), chief information security officer (CISO), or other executive.

If OT systems have been in place and virtually unchanged for decades, software components may be minimal and thus there may not be additional value brought by the IT department. However, vendor risk management could create an opportunity to launch a discussion with each LOB manager.

Figure 1 | Impacts and Recommendations for CIOs and IT/OT Vendor Risk Management

Impacts	Top Recommendations
OT vendors lack experience in addressing software life cycle and security management processes, and consequently introduce vulnerabilities to enterprises.	• Spearhead IT/OT executive steering committees and implement vendor risk management task forces, assigning liaisons to each affected line of business.
Issues around authority, organizational boundaries and lack of trust prevent enterprises from adopting standardized vendor risk management practices.	• Get involved in (not take over) vendor risk management activities and raise awareness of OT vendor risks.
Due to a lack of sharing, transparency and accountability, many common OT vulnerabilities are unknown to the enterprise and remain unmonitored.	• Sponsor, prioritize and ensure vendor risk management disciplines are adequately funded to increase maturity levels and mitigate enterprise vendor risks.
Many OT vendor risk management programs are either nonexistent or too immature to adequately and effectively mitigate enterprise-class vendor risks.	• Standardize vendor risk management programs as ongoing disciplines across the IT/OT spectrum, providing risk assessment, contracting strategies, monitoring and mitigation efforts.

OT = operational technology
Source: Gartner (March 2014)

Impacts and Recommendations

OT vendors lack experience in addressing software life cycle and security management processes, and consequently introduce vulnerabilities to enterprises — CIOs are uniquely positioned to help manage these vendor risks across the entire IT/OT spectrum

Although not all OT vendors are the same, most OT vendors have not historically focused on the proactive measures of security and risk management normally found among IT vendors. OT vendors have fewer best practices, if any, in place to assist in network and software-related risk mitigation. It has also not been the focus of LOB leaders and engineering staff to source preferred OT vendors based on these capabilities. CIOs responsible for IT/OT converged technologies cannot rely upon the vendors (or the LOB) to mitigate risks. We have seen numerous attacks to both networks and endpoints of connected OT solutions. These instances of enterprise-class failures — and the data loss resulting from OT-software-related intrusions — will continue to increase until CIOs take the lead in developing vendor risk management programs that encompass both IT and OT technologies.

As OT vendors move toward being more software-enabled — using commercial or common platforms — they may improve some competencies and risk management practices. However, your specific set of vendors may not. Review your OT vendors' software management and delivery processes to determine the level of competency in these areas. Conducting formal due diligence on critical and strategic vendors is recommended and should be followed by ongoing tracking of risks through a vendor risk register.

Historically, contracts and purchase order agreements within the OT industry have been tied to overall equipment purchases, and are not typically seen as separate contracting elements. Terms and conditions and SLAs found in standard IT contracts are likely to be conspicuously missing in OT contracts. Negotiating T&Cs that provide the same protections found in IT vendor contracts will prove challenging and will be best handled by staff who have the expertise in negotiating similar clauses in IT agreements.

To ensure that vendor management (or IT procurement) staff have the contractual expertise to negotiate vendor risk clauses and monitor vendor risk — and also knowledge and understanding of the affected LOBs — consider a business partnering strategy. This would align LOBs with specifically identified personnel within vendor management teams who can act as dedicated liaisons. This will help to build trust with the LOB and the OT vendors. CIOs must work diligently to upgrade not only their vendor relationship management processes, but also internal relationship building skills in these areas.

Recommendations:

- Spearhead IT/OT executive steering committees and implement vendor risk management task forces — assigning liaisons to each affected LOB.
- Establish an IT/OT vendor risk governance group, composed of IT, procurement, enterprise risk management, and business unit leadership to establish your IT/OT vendor risk management program.
- Work with the LOBs to offer development of software-related OT contract T&Cs using resource-sharing of appropriate contract negotiation, or sourcing personnel.
- When working with the LOBs, engage in discussions about risk with OT vendors that are most critical or strategic to the enterprise. This is to understand their capabilities and willingness to participate/collaborate with risk mitigation activities.
- Work with vendor management teams to begin tracking OT vendor risks using a combined IT/OT vendor risk register.
- Accept accountability for all aspects of vendor risk management that are transitioned to the CIO for oversight — reporting activities and ongoing management results to affected LOB stakeholders and executive steering committees.

Issues around authority, organizational boundaries and lack of trust between CIOs and operations/engineering team leaders prevent enterprises from adopting standardized vendor risk management practices across the IT and OT vendor ecosystem

OT risks often remain unaddressed because the discussion about responsibility for vendor-related activities can be a politically charged topic. Often, the LOBs feel that the IT department is attempting to take over areas that have traditionally remained under the leadership of the LOB executives.

Also, LOB leaders might assume that their authority and expertise is in question. There is also an impression that the involvement of IT could create bottlenecks to execution, or worse — it could undermine the objectives and mission of each LOB through the restriction of access to needed technology, or the mismanagement of the respective applications.

Trust in the office of the CIO as a partner in executing OT strategies can depend on a number of factors, including:

- Enterprise culture
- Hierarchical placement within the enterprise
- Historical trends of success or failure by the CIO in addressing the needs of each LOB

Where IT departments are viewed only as purveyors of email and network connectivity, there is significant ground to cover in terms of building trust across LOB boundaries.

Ironically, although in some organizations the CIO may sometimes feel that they are the least-trusted executive in the enterprise, they are uniquely positioned to holistically address vendor risks to the enterprise. The CIO's team will have extensive experience with software vendors and visibility across all LOB network connections and endpoints. This is unlike LOB leaders who, because of the nature of their business expertise, are highly siloed.

To avoid duplication, redundancy and potentially being sidelined for future business decisions that may affect the enterprise, CIOs must engage with their LOB leaders regarding vendor risk management. A first step in this process is simply raising awareness about the real risks faced by the enterprise, and educating leaders about what can be done to mitigate them.

Where existing IT vendor risk management programs are in place, these can be modified and enhanced to include the monitoring of OT vendors. Often, the IT department (and its IT procurement, strategic sourcing or IT vendor management subgroups) is the only organization with the established and required skills, tools and experience for performing risk assessments, negotiating vendor contracts effectively and performing ongoing monitoring of vendor risk elements.

In addition to trust issues, to overcome the view that IT is merely a bottleneck to innovation or improving processes, CIOs may need to develop unique sets of risk-reward analysis for OT technologies that are completely different from IT parameters. Although IT processes can and should be leveraged, the methodology and decision matrices can be very different. Consider "fast track" programs for OT or digital business that route those requests through a separate team or office. Additionally, due diligence checklists can be developed that are unique to each LOB; for example, where growth targets are aggressive, innovation may trump risk mitigation. However, for other LOBs, regulations could dictate what level of vendor risk is/is not acceptable. Implementing these processes will discourage potential bypass of vendor risk management activities and can enable shorter cycle times and repeatable processes for OT vendor sourcing, contracting and performance monitoring. But ensure that a risk-reward analysis is completed in advance of awarding business to the applicable OT vendors — even if risk tolerance levels are different among the LOBs.

Often, it is not the LOB leaders themselves who begin to raise concerns about the ramifications of failure to monitor and mitigate OT risks. The CISO, CFO and CRO (and others such as asset risk managers) typically have the greater desire to address enterprise risks as these executives must report enterprise-level risks to the board. Our 2013 risk survey respondents indicated the most senior-level roles dedicated to IT risk management (see Figure 2).[2]

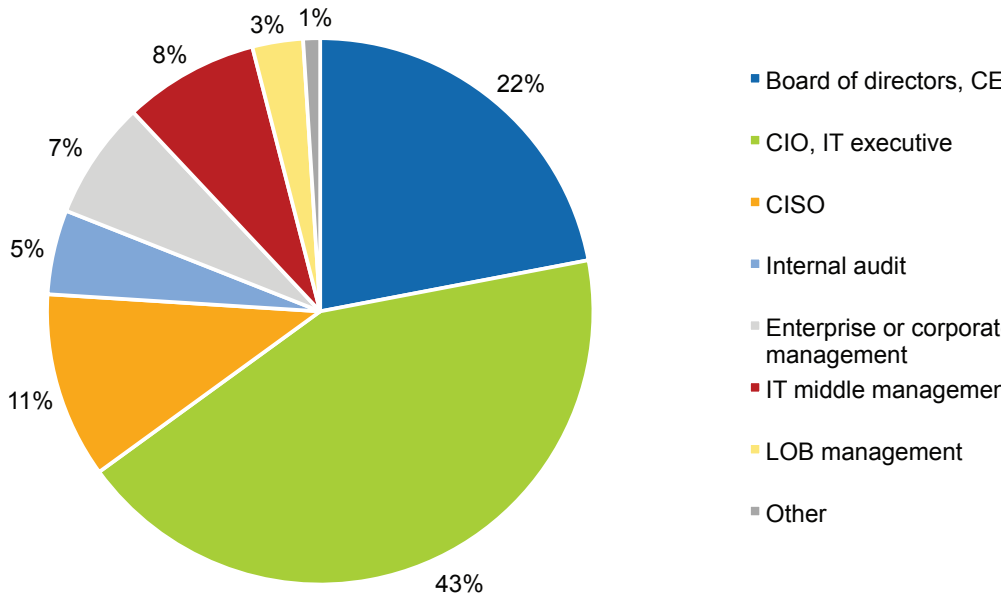
These results are based on this question: In your organization, to whom does the most senior-level person dedicated to IT risk management directly report?

In public companies, minimizing these risks is critical to corporate security ratings and shareholder opinion.

Recommendations:

- Get directly involved in (not necessarily take over) vendor risk management activities and raise awareness of OT vendor risks among LOB leaders.
- To avoid territorial responses, offer security and risk assessment services to the LOBs rather than suggesting a change in management of these activities.

Figure 2 | Reporting for Most Senior-Level Roles Dedicated to IT Risk Management



CISO = chief information security officer; LOB = line of business
These results are based on this question: In your organization, to whom does the most senior-level person dedicated to IT risk management directly report?

Source: Gartner (March 2014)

- Meet with your IT steering committee, the CRO, CFO and CEO to cite OT enterprise-class risks and opportunities that have resulted in negative consequences for other organizations.
- Consider fast-track programs for OT or digital business that route those requests through a separate team or office, using unique risk-reward analysis frameworks for each LOB.
- Conduct a pilot with amenable LOBs to assess enterprise risks through a formal audit of OT software and/or endpoints.
- Use the success of pilots to expand vendor risk management services to other LOBs.

Due to a lack of sharing, transparency and accountability among CIOs and operations/engineering team leaders, many common OT vulnerabilities are unknown to the enterprise and remain unmonitored — and could have potentially devastating consequences

When accountability is in question, often neither the CIO nor the LOB leaders take responsibility for OT vendor risk elements. Line-of-business leaders are focused on production and execution aspects of these technologies, and CIOs without designated authority are typically reluctant or disempowered to take action.

Although OT solutions are often attached to well-protected networks, we have seen that a highly secure network or even disconnection is not a panacea for avoiding attacks. For example, Stuxnet was not a networked vectored attack. OT solutions are sometimes connected or accessed by field technicians using mobile and other endpoint devices. Based on recent failures, enterprise-class intrusions and subsequent failures or breaches are as likely — if not more so — to be targeted at mobile devices and/or OT endpoints as they are to enterprise networks (see Note 1).

Unfortunately, this exposes the enterprise to blind-side risks that could have devastating consequences — consequences that could have been mitigated or avoided with a proper OT vendor risk management strategy.

The good news is that there are common issues among OT vendors and their related technologies. Becoming familiar with these issues and the methods used to mitigate them is a critical success factor in reducing this exposure to the enterprise.

In Table 1 we have outlined some of the more common OT vendor risk elements. Notably, these are highly dependent upon the industries and types of production environments involved, and will vary from organization to organization.

Table 1 | **Examples of OT Vendor Risk Vulnerabilities, Causes and Suggested Mitigations**

Vulnerability	Cause	Suggested Mitigation
No SLAs are in the contract.	OT vendor agreements are typically focused on terms related to delivery and performance, not ongoing support.	• Conduct due diligence to determine the level of SLAs you will require for each vendor. Require sourcing and/or contract negotiation teams to create standard boilerplate language for use in OT vendor contracts. • Require SLAs as part of sourcing evaluations. Ensure that ongoing monitoring of vendor adherence to the SLA is completed.
T&Cs are locked down.	Long-term contracts — seven years or more — often with autorenewal.	• As part of an OT vendor contract checklist, restrict acceptance of long-term contracts that do not provide the ability to terminate for convenience. Work to reduce contract length over time.
There is a failure to provide ongoing support of the current product/version.	Agility and speed to market for OT vendors has involved new versions of products without upgrade paths. The extended life cycle of production elements makes this difficult to address in the long term. Included in this are version upgrades of embedded products and OSs such as Microsoft Windows.	• Insert provisions into OT vendor contracts to require extended support or to provide access to source code for any software to be discontinued. • Ensure there are contractual obligations requiring OT vendors to maintain embedded software by installing all available patches and upgrades. • Consider using software source code escrow agreements to protect against product end-of-life situations and loss of support caused by insolvency.
There is a failure to adequately patch software and provide the necessary security mitigations. This creates additional layers of risk when IT/OT converge, due to exposure and linkage to IT components.	OT vendors have often not secured or updated their OT-based software as IT vendors would. This has not been a requirement from engineering staff.	• Require that vendors provide security patches for known malware. • Request warranties that software will be free of such malware during the agreement term.
		continued

Vulnerability	Cause	Suggested Mitigation
There are risks caused by embedded hardware components — which can affect functionality, support and product life cycles, and could raise import/export issues.	Third parties may provide components within the technology. The primary OT vendor may not accept responsibility for ongoing functionality of these component parts, including their respective OSs and databases.	• Request warranties for component parts for the entire life cycle of the technology. • Ensure the OT vendor is required to disclose the origins and suppliers of all component parts. • Insist on road maps of component parts that may need replacement and develop a mitigation plan as components reach their end of life.
There are no consistent BCM, backup or DR plans.	No standardization among OT vendors of these practices, where they exist.	• Require that all critical OT vendors participate in BCM and DR programs, and provide certification of adherence to these programs at least annually. • Acquire audit rights to evaluate committed standards of OT vendors, as needed.
There are competing formats for data storage, which leads to complexity, rising costs and increasing risks where multiple formats must be utilized.	Formats for storage vary widely based on the underlying technology. There has also been a focus on isolated rather than connected systems.	• Have sourcing staff identify options for storing OT vendor data. • Work with IT infrastructure staff to provide standardized practices to convert and migrate data into standardized formats where possible.
There is a lack of data security provisioning at both the network and endpoint levels, which can expose the enterprise to malware, data breaches, data loss and RAM scraping.	No historical focus from OT vendors on software and security concerns. Clients may assume the product is isolated from the network and therefore inherently protected.	• Ensure that sourcing teams obtain information about the full extent of OT vendor capabilities in this area. • Identify gaps where vendors will not provide adequate protections. Where gaps exist, assign mitigation activities to qualified internal staff to address vulnerabilities, and monitor them proactively.
There is a lack of value chain visibility, which can cause failures, and brand reputation, supply, geopolitical and financial risks.	Although this is becoming a greater focus in highly regulated industries, it has not been a historical focus for OT sourcing.	• Require transparency and full disclosure of value chain partnerships and affiliations of OT vendors. • Develop an ongoing discipline to sustainably monitor critical OT vendor linkages, affiliations and downstream providers.
New, niche and innovative, specialized vendors that have not been vetted over time, which increases insolvency and M&A risks.	Demand for innovation is driving sourcing beyond the more established vendors. Highly specialized OT vendors create competitive advantage for enterprises.	• As part of business continuity planning, ensure there are plans to migrate to other vendors — or to move support for OT applications and technology in-house — should a failure or M&A activity occur

Source: Gartner (March 2014)

Recommendations:

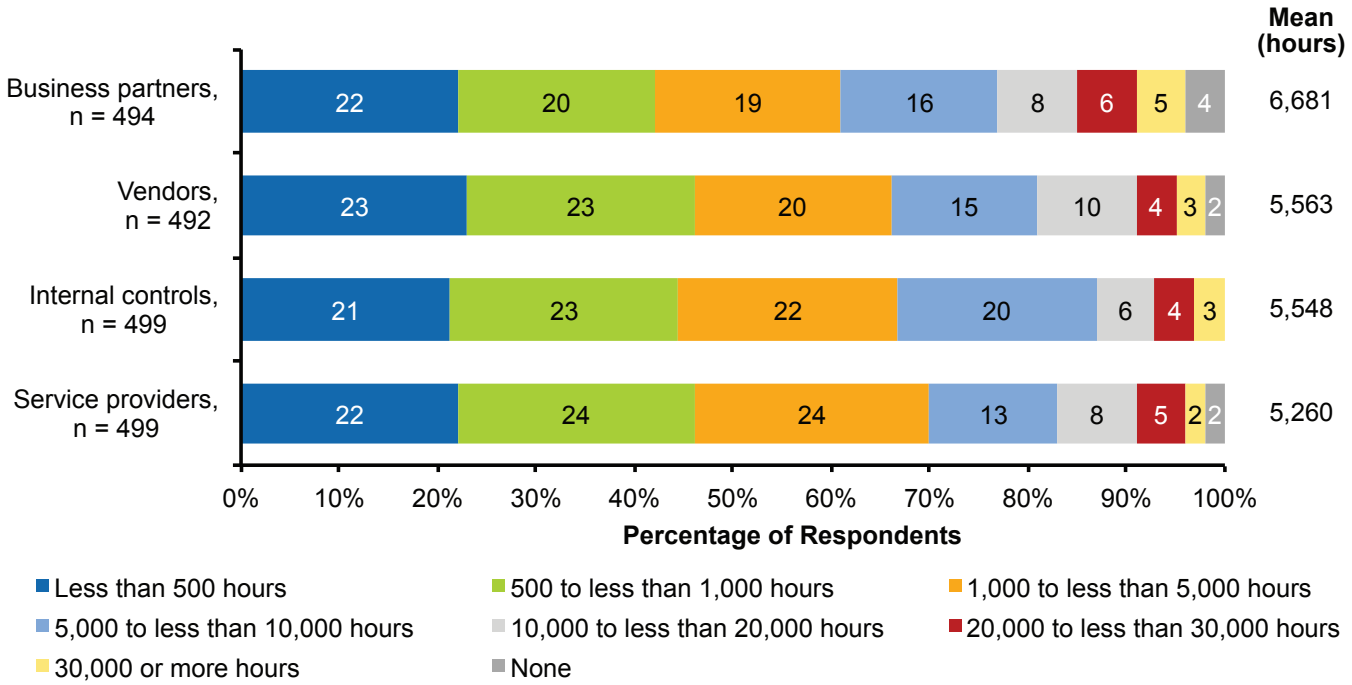
- Sponsor, prioritize and ensure vendor risk management disciplines are adequately funded — to increase maturity levels and effectively mitigate enterprise vendor risks.
- Use the vulnerability column in Table 1 to help identify current areas of OT vendor risk exposure, and express the need to establish clear ownership of these vulnerability assessments/ mitigations.
- Map vulnerabilities and mitigation activities to the available skill sets within IT. This is to stress the advantages of either housing appropriate aspects of the OT vendor risk discipline within the office of the CIO, or linking with IT team members who can assist in OT vendor risk management.

Many OT vendor risk management programs are either nonexistent or too immature to enable CIOs to adequately and effectively mitigate enterprise-class vendor risks

Vendor risk management itself is an immature discipline within IT vendor management organizations. Among IT those vendor management professionals surveyed, approximately only 10% had formalized ongoing risk management programs.[3] At best, risk reviews are undertaken during the sourcing phase to test the financial viability of vendor candidates. Even those organizations that monitor ongoing vendor risk management may still review only financial concerns using out-of-date sources with historical views, rather than proactively attempting to predict and mitigate other types of failures.

Even in organizations with formal enterprise risk management departments, third-party risk management is not usually a high priority. In our 2013 risk survey, respondents indicated the number of staff-hours spent on internal and external controls related to third-party risk management (see Figure 3).[4] The results show that this may be an afterthought for many enterprises.

Figure 3 | Hours Spent on Assessing Internal/External Controls



These results are based on this question: How many staff-hours (total per annum) do you estimate your organization spends on assessing internal controls and external controls of service providers, vendors and business partners?

Source: Gartner (March 2014)

This leaves enterprises exposed across the entire vendor ecosystem to unforeseen and unmitigated risks that could lead to enterprise-class failures. Because of the increasing industry and country-based regulatory requirements, this lack or inadequacy of vendor risk management processes could lead to noncompliance, fines and sanctions on enterprises that fail to address them (see Note 2).

As C-level executives, CIOs must be mindful of risks that could affect their enterprises as a whole, particularly those related to IT/OT, and take steps to mitigate that risk. Additionally, CIOs should be looking for opportunities for the IT organization to provide business value even when it may not be currently doing so. IT and OT risks should be evaluated simultaneously as part of an overall vendor risk management initiative. If there is no executive owner of this responsibility — such as a CRO or CISO — or if IT/OT risks are not covered under existing risk disciplines, the CIO must take action.

Recommendations:

- Standardize vendor risk management programs as ongoing disciplines across the IT/OT spectrum — providing risk assessment, contracting strategies, monitoring and mitigation efforts.
- Where no ownership of vendor risk exists, take the initiative to sponsor enterprise vendor risk management, elevating the importance of the discipline.
- Have the appropriate teams in your organization work with the LOBs to conduct formal risk assessments and develop strategies to address the OT risks. Do this by using new standards for OT vendor contracts, risk monitoring and risk mitigation that align with similar strategies implemented with IT vendors.

Acronym Key and Glossary Terms

OT	Operational technology is hardware and software that detects or causes a change of state in enterprise equipment; for example, industrial control and sensing technology. OT systems were previously hard-wired systems, electromechanical systems, and proprietary single-purpose or stand-alone systems, but are now being replaced by more-complex OT software and firmware products that create a more-complex digital business for those affected. As OT products change and take on more commercial software infrastructure and underpinnings, the governance of the OT portfolio becomes more complex and presents software management challenges. Also, OT is part of a larger world of digital technologies and the industrial subset of the Internet of Things (IoT). Although there are consumer and product components that are part of the IoT, this research document concentrates on those that impinge on commercial, enterprise and industrial operations. Within that space, there is a subset of software systems that control or detect the state of physical assets in many enterprises. This is what we refer to as "operational technology." Because of their nature, OT systems are usually provided by outside specialists as software products linked to equipment. However, these specialists have begun to experience the volatility and changeability of software in the IT world, as the underlying technology of OT converges with IT.

Evidence

[1]In the 24-month period ending 31 December 2013, Gartner IT/OT analysts conducted over 280 client interactions, including discussions around OT risk and security.

[2]In the 24-month period ending 31 December 2013, Gartner security and risk analysts conducted over 1,490 client interactions, including third-party risk management calls.

[3]Informal polling of attendees at the Gartner outsourcing and vendor relationships, ITAM, and business activity monitoring summits (2011 to 2013) indicated that approximately 10% of organizations are performing ongoing, repetitive vendor risk management. This is unlike one-time due diligence efforts, which almost 100% of organizations conducted.

[4]Gartner surveyed a total of 555 organizations in four countries — between 24 April 2013 and 10 May 2013 — to help it understand how risk management planning, operations, budgeting and buying are performed. This was particularly in areas such as risk management, information security, business continuity management, IT compliance, and privacy.

In all, 555 respondents participated from the U.S. (N = 151), Canada (N = 102), the U.K. (N = 151) and Germany (N = 151). Country and risk management discipline area quotas were established to enable the comparison and contrasting of key trends. Organizations from all industries qualified. Factors that were part of the survey are as follows:

- Qualifying organizations were large organizations with at least $50 million equivalent in total annual revenue for fiscal year 2012.
- Qualified participants must have reported being extremely involved in one of five risk management disciplines, or be team members in two of five areas.
- Interviews were conducted online and in the native language (English or German). The sample universe was drawn from external panels of IT management professionals.
- The survey was developed collaboratively by a team of Gartner analysts who follow the IT market and was reviewed, tested and administered by Gartner's research data analytics team.

Note 1. Examples of IT/OT Software Threats

The following are examples of software threats:

- "Stuxnet"
- "Duqu"
- "Flame (malware)"
- Gauss (see "Custom Font Flags Computers Infected With the Gauss Virus, Cousin of Stuxnet," Wired, 13 August 2012)
- Red October, see "Hunt for the Red October Virus: Top 10 Facts You Need to Know" (Heavy, 15 January 2013) and "The 'Red October' Campaign — An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies" (securelist.com)
- "Prof" — password theft (see "SCADA Systems at the Water Utilities in Illinois, Houston, Hacked," ZDNet, 21 November 2011)
- Target credit card exposure (see "Target Hackers Broke in Via HVAC Company," KrebsonSecurity, February 2014)
- Sensor node risk (see "Software Maintenance of Deployed Wireless Sensor Nodes for Structural Health Monitoring Systems," Quadri, S.A. and Sidek, O., International Journal of Computer Engineering Science (IJCES), Volume 3, Issue 2, February 2013)

Note 2. Examples of Regulatory Involvement in the Security of Critical Infrastructure

- "Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection," 17 December 2003, U.S. Department of Homeland Security.
- "Digital Agenda: European Commission Supports Research on Cyber Security," Memo/12/899, 26 November 2012.
- "Presidential Policy Directive/PPD-21 — Critical Infrastructure Security and Resilience," The White House, 12 February 2013.
- See also "Market Trends: Critical Infrastructure Protection, Worldwide, 2013."

Source: Gartner RAS Core Research Note G00261054, G0

About Positive Technologies

Positive Technologies is a leading provider of vulnerability assessment, compliance management and threat analysis solutions to more than 1,000 global enterprise clients. We are among the world's most advanced specialist researchers, renowned security experts and highly-skilled programmers.

With one of the largest and most dynamic research facilities in the world, Positive Technologies carries out research, penetration testing and threat and vulnerability analysis on dozens of large-scale networks each year. As a result we have developed a unique understanding of how security should work, across a wide range of geographies and systems. We earned our reputation as one of the foremost authorities on SCADA, Banking, Telecom, Web Application and ERP security, anywhere.

Our solutions work seamlessly across your entire business: securing applications in development; assessing your network and application vulnerabilities; assuring your company's compliance with regulatory requirements and corporate standards; and blocking real-time attacks. Positive Technologies will give you complete confidence in the security of your network, its associated policies and its related applications.

Hands-on experience, underscored by a decade of service to clients worldwide, has enabled Positive Technologies to develop a thorough knowledge and understanding of vulnerability and compliance management that is unmatched. Our commitment to clients and track record of research excellence has earned Positive Technologies distinction as one of the fastest growing Security and Vulnerability Management firms in in the world.

To learn more about Positive Technologies please visit www.ptsecurity.com