
Hacker
Computer
Hackerkultur
Subkultur
Begriff
Bearbeiten
Computersicherheit
wurde
Eric
Weitere
entwickelte
Hackerbegriff
Hackerszene
Teil
wurden
Freie
Verwendung
Hackern
Lösung
Jahren
Jargon
Mitte
Bezeichnung
Subkulturen
Source
jemand
Entwicklung
hacking später
stark
Manipulation
Abgrenzung
Umfeld
gang
Technologie
außerhalb
Spaß
maßgeblich
ursprünglich
Aktivitäten
Rechner
File
to
einfache
Heroes
How
Motivation
1970er
allgemein
Homebrew
CCC
seit
sehen
gibt
Daran
become
besonders
Homecomputerszene
tmrc.mit.edu
Programmierer
Fall
Telepolis
by
Hauptartikel
gab
gilt
Siehe
Software
hardware
Weise
press
at
1950er
Heimcomputer
allgemeinen
Umgehung
Wort
Club
Bereich
Phreaking
Hackers
Innerhalb
Revolution
Selbstverständnis
findet
Person
Gründahl
Beispiel
hack
Kontext
Industrie
Art
Cracker
insbesondere
erste
entwickelten
Thompson
deren
1980er
Personen
frühen
1990er
ersten
Vermittlungsstellen
Computers
zunächst
The
of
akademischen
and
dabei
Open
denen
Free
bezeichnet
Hackergemeinschaft
Jahre
Raymond
meist
Sicherheitsmechanismen
steht
darauf
wobei
akademische
Kultur
Hacken
system
on
sowie
Levy
Zusammen
abhängig
geprägt
Jargon-File
Anhänger
Zugriff
Sinn
TMRC
Steven
allerdings
allgemeiner
technischen
Technik
Bewegung
ISBN
AI
beschreibt
Internet

ARE CYBERSECURITY RISKS LURKING IN YOUR Supply Chain?

By Timothy Hall

Business leaders need to establish a common, companywide defense to handle the ever-changing threat of cybersecurity attacks.

Cybersecurity is among the top concerns facing businesses today — no real surprise, given the number of highly publicized data breaches, distributed denial of service (DDOS) attacks, and the growing cost and complexity of fixing these problems.

With the proprietary design, pricing and contract intelligence that flow through complex supply chains, supply management organizations must account for and address the cybersecurity risks in their operational planning and execution. This seemingly simple task requires supply management leaders to understand and balance operational performance opportunities and cybersecurity risk trade-offs within current business plans.

It's Everyone's Business

It's easy and tempting to relegate the responsibility of cybersecurity risk to the chief information officer or the chief risk officer. In reality, the risk is impacted by virtually every employee, process and technology decision made by operational managers. Too often, businesses are under the misperception that cybercrimes only happens to large companies. However, any company with a competitive advantage, desirable technology, financial access or proprietary insight — and suppliers to those companies — are targets.

While the majority of cybercrimes are financially oriented, there is a growing organized-crime and nation-state supported threat directed at increasing the competitive position of an industry through the collection and exploitation of proprietary and competitive information.

For a broad range of these organized threats, cyberbased information collection has become the method of choice for several reasons:

- **It's cheap and easy.** Sophisticated attack tools are easily accessible at hacker sites and require little expertise to use.
- **It's fast.** The very nature of the technology allows the attacker to quickly transfer vast amounts of information, and once your information is out, you can't get it back.
- **It's nearly undetectable and un-attributable.** The ability of attackers to remove digital fingerprints, the increasing similarity between the tools, tactics and techniques used by various attackers, and the ability to mask geographic location in cyberspace make it difficult to definitively assign blame.

Adversaries realize that coordination and information-sharing practices provide excellent exploitation paths up and down the supply chain. In other words, if they can't easily get into the primary target, they attack members

ARE CYBERSECURITY RISKS LURKING IN YOUR

Supply Chain?

of the supply chain and access the primary target through trusted communication links. With the trend toward supplier integration and supply intelligence, it's easy to understand that the supply chain has moved to the head of the class as an industrial target.

Tipping the Scales

On one side of the equation, there is a dedicated adversary with effective exploitation tools looking for a target, and on the other side is a company with a wealth of information stored in its networks and a communication path to other supply chain partners. Currently, the advantage clearly belongs to the aggressor. The question is how to start tipping the scales toward the good guys.

While executives and operational managers drive decisions to optimize performance and profitability, many are not aware how their decisions affect the company's overall cybersecurity risk position. They typically delegate the management and control of this critical risk area to technology leaders, who often operate outside the day-to-day business decision matrix. Too often, the coordination and optimization between business leaders driving business and technology leaders driving technology is lost due to lack of common goals as well as the ability to communicate technical challenges and objectives.

Current and evolving regulations require business leaders to attest to the integrity and appropriateness of the organization's controls. The CIO can provide assurances that security measures are operating according to plan, but without a common, baseline understanding of cybersecurity, it is difficult for the supply chain practitioner to know if those assurances translate to his or her perception of the controls. Traditionally, business leaders rely on benchmarks or traditional security assessments to validate those assurances, but such measures can be time-consuming and expensive.

There are several low-cost, manageable steps that can demystify the cybersecurity risk discussion. These steps also will help you validate your organization's perceived risk position and reduce its supply chain's exposure. They include:

1) Establishing a common understanding of the interdependence and impact of operational business decisions on cybersecurity
2) Conducting a focused assessment to validate your organization's perceived risk position and form a basis to prioritize investment and implementation strategies
3) Integrating enterprise leadership and the supply chain into a coordinated solution to deter and handle cybersecurity issues.

Finding Common Ground

Company executives are becoming acutely aware of cybersecurity risks. However, there is often a gap between the technical (CIO, CISO) and business (CEO, CFO, CPO) leaders' understanding of the risk. The arcane nature of cybersecurity prevents most management teams from sharing a common understanding and appreciation of questions such as:

- Which cybersecurity risks apply to them?
- What type of events are likely to occur?
- How will these events manifest themselves?
- How will cyberattacks most likely be discovered?

What protection, detection and forensics capabilities can be expected from current security technology and process controls?

A Pell Center study by Francesca Spidalieri about leadership in the cyber age found most of today's business leaders earned degrees in fields other than computer network security. Few understand what cyberspace is, how networks physically work, and the connections between operational decisions and the dangers that lurk within cyberspace.

Conversely, industry IT experts tend to be principally concerned with technical solutions to cybersecurity problems. However, cybersecurity risk management requires not only IT experts with computer science, electrical engineering and software security skills, but also professionals with an understanding of business theory, organizational structure, behavioral psychology, ethics, international law and enterprise risk management.

Understanding Cybersecurity Links

Bridging the technical and business sides of this complicated problem is critical if senior leadership is to effectively provide cybersecurity oversight and guidance in the areas of IT acquisition, adoption of business applications and processes, cybersecurity budgets and IT outsourcing.

Without a common baseline understanding of the size, cost and complexity of the cyberthreat, and the remediation and transfer options available to the organization, it is difficult to truly appreciate and scope your organization's risk profile. To make matters worse, without a common orientation, the response and remediation may not be satisfactory when a cybersecurity event occurs.

For example, when the CEO wants to know exactly how long an adversary has been on the system or exactly what was taken, it would be more productive if he or she understood basic cyberforensic capabilities and limitations.

Technical proficiency is not the objective. Operational managers should be educated about the links among business decisions, cybersecurity vulnerabilities, and mitigation techniques and limitations. Cyberattacks will likely overwhelm a company's capacity to properly respond and protect its assets. Establishing a common understanding of senior management's cybersecurity-related roles and responsibilities,

as well as the interdependencies among business units and cybersecurity decisions, will better position the leadership to plan, prioritize and react when an event occurs.

Evaluating the Risk Position

A recent blog posed the question, "How do you respond to the CEO when he or she asks: 'Are we secure?'" The answers varied from complex and detailed responses to "as secure as we can be for the money and resources we have."

It is tough to answer the question because of all the nuances associated with it, such as what is meant by "secure," how secure is secure enough, how is security measured and what does it take to be secure and maintain security.

The best way to address the question is to describe the organization's cybersecurity risk position. Risk is determined by effectively assessing the value of the resource, scoping the threats and vulnerabilities, determining the likelihood of an event and estimating the cost to mitigate the risk. Unfortunately, this seemingly straightforward task can be daunting.

Business functions and associated security controls are inextricably linked. The risk position is a result of a series of trade-offs between the needs of often opposing requirements, such as the need to share information and the need to protect information. To manage the cybersecurity risk of a business unit, including supply management, the business unit leaders, IT and risk managers should have:

- A common understanding of critical and valued assets
- An appreciation for the current and most likely cybersecurity threats and system vulnerabilities
- A candid assessment of the implementation and coordination of security controls
- An understanding of the breadth and scope of all of the byproducts of a cybersecurity attack and the true cost to remediate potential exploitations.

With this common understanding, business unit leaders can work together to effectively quantify risks, evaluate options and develop a cost-benefit analysis. A cross-functional team can then determine which risks should be accepted, mitigated or transferred.

A Focused Assessment

With the interdependencies among business units, applications and processes, and the constantly changing business requirements and cybersecurity threats, decisions and trade-offs need to be frequently re-evaluated. Using a traditional security assessment process to test your perception of current cybersecurity risk is a fairly costly and time-consuming process, especially for a large company.

Business leaders, however, can perform a focused assessment, targeted at one or more key business systems, to validate their perceived risk position and serve as an indicator of bigger challenges.

These assessments should target a system that is consistent with current threat intelligence and of interest to the anticipated adversary, deals with critical resources, crosses enterprise boundaries and coordinates with external partners.

The focused assessment should at least consist of:

1) Reviewing system and subsystem security architecture
2) Sample testing, using representative exploitation tools and simulating anticipated network attacks such as website attacks, DDOS, and access and authorization
3) Reviewing hierarchical implementation of security controls
4) Using and integrating contingency, emergency and disaster recovery plans.

The targeted analysis will help determine whether business applications and security controls are integrated, coordinated and maintained as an integral part of the larger IT infrastructure. This sampling also can quickly identify any serious gaps and serve as an indicator of potential broader cybersecurity risk concerns.

Strategy Trumps Tools

Today's supply chains are providing industrial partners and sophisticated adversaries access to huge amounts of proprietary information and intellectual property. The appetite for trade secrets and competitive information coupled with current attack methodology guarantees that all organizations, regardless of size, are targets.

Billions of dollars are spent every year developing and implementing products, processes and technologies to address this continually evolving risk. There are many security products available that will reduce your company's exposure and increase its ability to respond to a cyberevent. However, a coordinated cybersecurity/business strategy is more important than individual tools. Unfortunately, most management teams lack a common cybersecurity/business risk framework to enable effective trade-offs and prioritize technology investments and integration.

Establishing a common understanding of cybersecurity risk and its links to organizational objectives and business decisions will better position executive leadership to strategize, prioritize, plan and react in real time when a cybersecurity event occurs. **ISM**

Timothy Hall is president of AZORCA Cyber Security, LLC in Millersville, Maryland. For more information, send an email to **author@ism.ws**.