Making Everything Easier!™

Cisco Special Edition

Trustworthy IT Business Partners

FOR DUMMIES®

A Wiley Brand

Learn to:

- Identify trustworthy IT business partners
- Recognize the policies that build trust
- Know what you need to protect

Brought to you by

CISCO™

Brian Underdahl

Trustworthy IT Business Partners

FOR DUMMIES®
A Wiley Brand

Cisco Special Edition

by Brian Underdahl

FOR DUMMIES®
A Wiley Brand

Trustworthy IT Business Partners For Dummies®, Cisco Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN 978-1-119- 10214-4 (pbk); ISBN 978-1-119- 10209-0 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Editor: Jen Bingham

Acquisitions Editor: Katie Mohr

Editorial Manager: Rev Mengle

Business Development Representative: Karen Hattan

Introduction

Why does your company trust the IT products it uses? Because the products work as advertised, the brand name is one you implicitly believe in for any number of reasons, or the product was tested and passed the tests? Is it because everyone else is using it so it must be okay; when something goes wrong, the company that produced it fixes it; or you asked how something was built, where it was built, and have proof? Any of these could be your reason to trust a vendor, or you could just be confused about which companies and products to trust. This book discusses what makes a trustworthy IT business partner — from secure development life cycles, vulnerability product testing, a published remediation process, investment in product resilience, supply chain security, to transparency, and ultimately, provable trustworthiness.

About This Book

This book shows you what you need to know as you evaluate IT business partners to provide devices and systems you need to help run your organization in a secure manner.

The routers, switches, servers, voice over IP systems, and other network services are the heart of your business as they provide the backbone of your infrastructure. These devices and systems are responsible for not only transmitting critical business data but must also help ensure the security of your business and its sensitive data.

Choosing your IT infrastructure partner in this age of attacks from criminals, nation states, political hackers, and insiders requires knowing the scope and depth of the vendor's security processes, policies, and technologies as well as understanding its commitment to security within its business culture.

Along the way, you'll see that security can no longer be provided with a point product or exist solely at the perimeter. Rather, security must be embedded into each product as well as within the organizational mindset. Products need to protect themselves as well as the data being transported, processed, and/or stored by your systems.

Icons Used in This Book

This book uses the following icons to call your attention to information you may find helpful in particular ways.

REMEMBER

The information marked by this icon is important. It helps you easily spot noteworthy information.

TIP

This icon points out extra-helpful information.

TECHNICAL STUFF

This icon marks places where technical matters, such as jargon and what not, are discussed. Sorry, it can't be helped, but it's intended to be helpful.

WARNING!

Paragraphs marked with the Warning icon call attention to common pitfalls that you may encounter.

Beyond the Book

You can find additional information about Cisco's take on finding trustworthy vendors by visiting `https://trust.cisco.com`.

Chapter 1

Introducing the Idea of Trustworthy IT Business Partners

In This Chapter

- ▶ Getting to know trustworthy systems
- ▶ Looking at what it takes to be a trustworthy business partner

The world has come to depend on data networks, especially the Internet, to support essential services. Both private and public organizations need to deliver services using a foundation of trustworthy information systems. Building trust into information technology itself is the best way to get there.

Trustworthy solutions provide continuously improved, evolving security designed to effectively anticipate and deter attackers. The creation and operation of trustworthy systems require the efforts of equally trustworthy business partners.

Not all vendors are qualified, willing, or able to develop trustworthy systems. Vendors aren’t inherently wicked, but trustworthiness is a new concept and relatively few vendors have cultivated the discipline required to make, sell, support, and validate the bona fides of trustworthy systems. Trustworthiness also must include accountability and transparency throughout product life cycles.

This chapter provides an introduction to the concept of trustworthy IT business partners and provides a brief background of what it takes to ensure the delivery of trustworthy systems.

Understanding Trustworthy Systems

Vital public and private services, infrastructure, and institutions all rely on the availability and trustworthiness of local and global data networks. No matter how you access networked services, you need to trust the information you access along with the systems that deliver them.

The very richness and openness of the Internet creates the motive and opportunity for malicious actors to misuse and misappropriate network-borne data, services, and resources. Even those who strive to add value to the network experience can inadvertently enable harmful behaviors. For example, social media companies offer free services to users but in exchange they harvest data about their users that can be stolen by attackers. Other organizations may bypass security checks and balances to rush a new service to market. The harvested data and bypassed security checks leave users open to exploitation. It's these types of problems that make securing the network and its data so important to today's users.

REMEMBER

Creating a truly secure infrastructure becomes even more complex as you invest in mobility, collaboration, cloud computing, embedded systems, and virtualization. These capabilities improve resiliency, increase efficiency, and reduce costs, but also introduce additional risks. The security of IT product manufacturing processes is also an issue, with counterfeit and tampered products being an ongoing problem. As a result, today's government and corporate leaders overwhelmingly identify cybersecurity, data protection, and associated trust issues as top concerns.

Seeing what makes up trustworthy solutions

Clearly, your organization needs to be sure that you can trust the systems and vendors you use to build your infrastructure. But how can you identify trustworthy solutions that will keep your organization safe? Here are some important characteristics that differentiate trustworthy solutions:

- **Trustworthy solutions incorporate built-in network security features and functions:** Defending against the rapidly evolving body of threats requires the capability to secure business infrastructure and data through protections built directly into IT infrastructures. The days of treating security as an overlay on top of universal machine computing processes are over. Business partners need to set trustworthiness as a design goal in product development. They must also back this goal with appropriate and effective trustworthiness-directed design review and revision processes.

- **Built-in trustworthy features include state-of-the art security technologies:** Trustworthy solutions incorporate security-focused features and functions that go beyond those found in generic equivalents. These features provide an enhancement to feature sets such as encrypted storage that harden products and avoid design errors that increase product vulnerabilities to external attack.

- **Trustworthy solutions comply with industry and government security standards relevant to customer business requirements:** Depending on your industry, you may need to comply with standards such as international Common Criteria standards, the Federal Information Processing Standard (FIPS) 140-2, Federal Information Security Management Act (FISMA), the Health Insurance Portability Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), or European Model Clauses (EUMC).

- **Trustworthy IT partners take steps to secure the integrity of their product manufacturing and distribution supply chains:** Trustworthy IT partners take care to maintain the integrity of their products against counterfeiting and tampering in the manufacturing and distribution processes. This process can include authenticity and tampering protections embedded into products in addition to external procedural controls and audits.

- **Trustworthy IT partners stand behind trustworthy solutions, and are always ready to validate features, functionality, supply chain integrity, and business practices:** No matter how strong the security features and operational processes embedded into a network may be,

> you can't trust the output of a networked system unless you can trust the vendors and service providers responsible for the system. Trustworthiness is easy to claim, but difficult to prove.
>
> Trustworthiness begins with transparency as the defining virtue of a truly trustworthy partner. Vendors must candidly reveal their processes for building secure products, enabling secure network architectures, ensuring data protection, protecting the integrity of manufacturing products, and delivering long-term solution maintenance and support.

WARNING!

Trustworthiness isn't an extra option you can add on after the fact. Unless the entire product cycle from concept, through design, and into implementation was centered on being trustworthy at each step, you run the risk of engaging with a product that might have dangerous security lapses or other potential and unanticipated holes that leave you vulnerable.

Trustworthy IT partners understand certain realities about gaining and maintaining trust. These include:

- Trust is earned; it can't be bought.
- It takes time and effort to earn trust, but it can quickly be lost.
- Earning trust is an ongoing effort.
- You can't control all factors; there are forces beyond your control.
- You must control what you can; always act in a trustworthy way.
- Be prepared for what you can't control.

Considering the trustworthy life cycle

Trustworthy systems need a continuous improvement approach to security that anticipates and preempts new threats. This approach not only protects your critical information, but more importantly, helps to avoid interruptions of critical services. Trustworthy solutions enable you to minimize the costs and reputation damage stemming from information misappropriation, service outages, and information or data loss breaches.

WARNING!

Simply owning trustworthy systems shouldn't be confused with immunity from external attack. You have an important role to play in maintaining the effectiveness of trustworthy systems in fending off attempts to breach your network. This includes activities such as installation of security-focused updates and patches, constant vigilance in recognizing abnormal system behavior, security awareness training of your employees, and effective countermeasures against attacks.

Technologies don't stand still — and neither do attackers. System trustworthiness needs to cover the full life cycle of an infrastructure from initial design through to manufacturing, system integration, daily operation, maintenance and updates, and even decommissioning of the solution.

Choosing Trustworthy Business Partners

You have to choose the right IT business partner. Choosing a truly trustworthy vendor marks a significant step toward maximizing the returns of your information technology system over its lifetime. Choosing the wrong vendor can significantly damage your enterprise information security and degrade overall return on information technology investment.

Although almost all vendors claim trustworthiness, partner transparency is the first and most telling indicator of trustworthy behavior. Trustworthy vendors don't hesitate to offer clear and independently verifiable information regarding things such as secure product development methodologies and practices, solution architecture precepts and techniques, manufacturing supply chain security, and post-installation system maintenance and support practices.

You get what you pay for in trustworthy systems. Organizations that make network technology investment decisions based solely on low-cost bidder criteria often rationalize this on perceptions of a low probability against an attack on their particular infrastructure, plus a belief that any attacks that have occurred have proven to be relatively mild.

WARNING!

This line of thinking ignores the risks posed by data security breaches and the growing destructive capabilities of hackers. It also downplays the vulnerabilities enabled by the shift to mobility, cloud computing, social media, and other new technologies. Experience has shown that any new technology carries with it vulnerabilities unforeseen by its developers.

Instead of setting aside these dangers, seek out business partners who see the risks as real and who have taken steps to create products and services that will protect your company.

TIP

Look for business partners that are transparent about security processes. You need and should require visibility into the following areas:

- Vendor product design, validation, and manufacturing processes
- Data protection
- Supply chain management
- Outsourced product quality assurance
- Cryptography policies
- Other factors relevant to system trustworthiness

Most vendors don't provide this information, nor do they have organized, end-to-end programs to document trustworthiness, largely because most IT customers have not yet demanded this level of disclosure.

Chapter 2

Identifying Trustworthy IT Business Partners

In This Chapter

- Looking at transparency
- Considering vendor accountability
- Understanding the need for leadership

The online world has become a far more dangerous place in recent years. Security and data breaches are a daily occurrence. Organizations of all sizes deal with increased numbers of cyberattacks. These dangers mean you need to find trustworthy IT partners whose products and services can help protect against all of these threats.

Unfortunately, the level of trust that people have for corporations has eroded over the past several years. In fact, according to a recent poll, global companies are among the least trusted groups in modern society. Obviously, these results aren't what a company that's trying to put forth a trustworthy image as a trustworthy business partner likes to see.

This chapter provides some guidelines to help you understand what characteristics to look for in a trustworthy IT partner.

Being Transparent

Trustworthy IT business partners must first be completely transparent with their clients. This transparency means being very open, having no hidden agenda, and delivering what they say they will. Vendors need to talk with all stakeholders in clear and straightforward language. And they must not make promises they can't deliver.

A trustworthy IT business partner is responsible and demonstrates integrity in all dealings with an organization's stakeholders including customers, employees, partners, investors, and society at large.

Some specific ways that trustworthy business partners can show they're behaving in a transparent manner include:

- Support of customers during physical disasters via a dedicated disaster response team
- Mandated customer data protection processes protecting customer data both in-house and at customer sites
- Having a required code of business conduct training and ethics training for all employees
- A policy of working with customers until a problem is resolved by owning the problem, its mitigation, and its solution.

One way to assess a vendor's trustworthiness is to look at how it deals with mistakes. Obviously, you want an IT partner who not only admits that a mistake or another problem exists, but that is also proactive in correcting the situation. You certainly don't want to deal with vendors that are always trying to pass off blame on someone else.

A trustworthy IT partner is transparent about its policies, processes, and technologies across its product lines. In addition, this transparency extends to all customer levels including any interactions with governmental agencies.

Being Accountable

You want an IT business partner that actually listens to customers and focuses solutions on their needs. Accountability includes being responsive and reliable.

Responsiveness goes beyond simply reacting quickly to your stated needs, however. A responsive vendor fully engages with you and anticipates needs you may not yet have considered. In this way, the vendor helps you solve IT challenges that you will encounter if you continue on your current path.

An accountable vendor works to build meaningful relationships and to become a trusted partner and advisor. Some of the ways it can accomplish this include:

- Managing customer problems with solutions and offerings that quickly resolve those problems
- Rapid response to vulnerabilities such as the recent Heartbleed exploit
- Clear communication of policies, processes, and incident management to effectively manage and address any actual or suspected data loss incident

Another foundation of a trustworthy IT partner is reliability. Reliability is about delivering products, services, and solutions that you can count on within an agreed upon time frame. And it also implies continuous improvement across products and services and staying up to date with the latest developments in the field.

Some examples of what to expect include:

- Explicit process, policy, and technology mandates for supply chain security
- A secure development life cycle for all products and solutions
- The insertion of trustworthy foundations into all platforms

Leading with Integrity

Another very important element in being a trustworthy IT partner is taking a position of leadership in protecting everything: its products, itself, and its customers. Leadership really means that the vendor has the expertise and vision to understand where the market is going and has the willingness to share that knowledge and provide solutions that protect before, during, and after an attack. You want a vendor who can anticipate upcoming challenges and technology changes in order to deal with them in a proactive manner.

Some specific signs of leadership include:

- Having a security baseline that provides stronger protection for a given use and threat model
- Creating a verifiable and transparent vulnerability handling process
- Continuous improvement and implementation of security baselines to cover an expanding threat landscape
- Focused research and proactive testing to find and mitigate vulnerabilities
- Product certifications with a common criteria protection profile for compliance and comparison
- Providing data security awareness training for everyone in the organization, not just for a specialized security team
- Sharing innovation for the benefit of all sectors

Chapter 3

Being Aware of What You're Protecting Against

In This Chapter

- Looking at perceptions
- Understanding the attackers
- Avoiding counterfeits and tampering
- Seeing the changing nature of threat disclosure
- Understanding threat types

It seems like every day brings more news about new cyberattacks. Major companies, governments, and even political activists have come under attack.

This chapter takes a look at the current threat landscape to help you better understand the changing types of threats and to give you an idea of the groups that are behind most of the attacks. By understanding the who and the why behind those threats, you can get a clearer picture of what you need to protect.

Understanding the Importance of Threat Perceptions

The recent news about the government's spying on almost everyone provides an excellent example of the importance of threat perceptions. Before Edward Snowden leaked thousands of documents to the press, most people probably didn't perceive a major threat to their personal data or privacy. Since that story broke, people have become aware that their phone calls and emails may no longer be private. But in addition to this feeling that their privacy is being invaded, many people have also lost faith in businesses that were alleged to have cooperated in some way with the government gathering their information. In other words, the mere allegations created a new perception that these companies were now also part of the threat.

Perceptions really do matter. Organizations often suffer from unfair assumptions that can result from careless media reporting when spectacular stories break. For example, when a news outlet uses stock footage showing computer or networking hardware to illustrate a story, many viewers take the implication that the hardware brands shown in that stock footage are somehow involved in the attacks mentioned in the story. It can be very difficult for vendors to "prove the negative" to viewers who believe the unjustified perception about the brand.

Looking at the Attackers

To truly understand the nature of today's cyberthreats, you need to know who's behind those attacks. This knowledge also helps you to better gauge which of your resources are most vulnerable.

Today's most common attackers include:

- **State actors:** These are the attackers who are part of or sponsored by a specific nation state. They have resources and their purpose is to steal intelligence information, disrupt operations, or steal intellectual property.
- **Organized crime:** This category includes the mafia, but not the mafia you may think of from television. Organized crime is focused on one thing: making money. It has extended its reach to the Internet because the risk is much lower than traditional criminal operations. These folks are into major fraud and theft activities, scareware, data breaches, credit card thefts, and online gambling. Most data thieves are professional criminals deliberately trying to steal information they can turn into cash.

- **Hacktivists:** These individuals are a new breed of attacker that is distributed, politically motivated, revenge oriented, and a general pain in the neck. The most well-known group calls itself Anonymous.
- **Terrorists:** These groups use computers just like everyone else — they exploit new technology to push their agenda forward. For example, Al-Qaeda's many uses for the Internet range from recruiting members and inciting violence to posting information on how to make bioweapons and forming social networks for aspiring terrorists.
- **Espionage specialists:** These people focus on stealing intellectual property from a competitor or with the intention of selling to the highest bidder.
- **Insiders:** Working from the inside -out, this is the thief who is hardest to detect and who could cause the most damage. Typically, this is an employee with legitimate access. This person may steal solely for personal gain, or she may be a spy — someone who is stealing company information or products in order to benefit another organization or country. Or, she may simply make a human error such as sending information to the wrong email address.

WARNING!

This list should certainly make you think about what you have to protect a little differently. You probably have assets that one or more of these groups of attackers would love to compromise.

Understanding the Dangers of Counterfeiting and Tampering

In addition to the types of attackers mentioned earlier, organizations also face real dangers from equipment that is either counterfeit or that has been tampered with. To understand why these issues can cause you harm, you need to understand the motivation of those who counterfeit or tamper with equipment.

Counterfeiters produce equipment that's intended to take advantage of the good reputation of brand-name products. Often, this counterfeit equipment looks very much like the real thing, but looks can be deceiving. For example, rather than using components that have been specifically checked and verified to make sure they meet electrical standards and will meet the specifications of the product, a counterfeiter uses the cheapest possible generic components. As a result, you risk getting equipment that doesn't contain all the security features that you expect from a major brand product.

WARNING!

A very common shortcoming in counterfeit networking products is ignoring the physical safety of the product. Often, units include improper fusing that can make them a fire hazard.

Just as counterfeit equipment poses a number of problems, equipment that's been tampered with can be very problematic, too. Illegal upgrades of a base product may be sold to gain the differential in price of the advanced product, leaving the product non-upgradeable when new software functions or maintenance is available. Equipment tampering also can focus on compromising the security features, as opposed to producing the cheapest possible product. For example, someone might tamper with networking hardware in order to install a backdoor or to insert a traffic monitoring software module. In any case, the purpose of the tampering is most likely to enable unauthorized data theft or monitoring.

TIP

Avoiding counterfeit or tampered equipment is relatively easy because all you have to do is to obtain your networking hardware from the manufacturer's official channels. Major manufacturers such as Cisco will generally stand behind any equipment purchased through these channels. Obviously, saving a few bucks buying from an unknown foreign vendor at an online auction site may have a certain appeal in times of tight budgets, but the risks involved are really too great to justify.

Seeing How Threat Disclosure Is Changing

It may seem a bit counterintuitive, but the trends in how threats have been disclosed over the past 10 to 15 years are having a major effect on the dangers posed to organizations by those threats. In fact, these trends mean that your data is at far greater risk than ever before.

Threat disclosure: 2000–2005

During this time frame, threats were often disclosed by security researchers directly to the vendor in exchange for a little fame while helping the IT community at large. The researcher might have wanted to do a presentation at one of the large security conferences such as DEFCON or Blackhat, and he almost certainly wanted to be able to update his resume. In most cases, however, these researchers weren't looking to directly profit from discovering the threat.

Another important feature of threat disclosure during that time frame was that researchers typically notified the vendor first and gave them time to correct the problem before making a public disclosure. As a result, manufacturers were able to correct problems before they became a security issue for equipment users.

Threat disclosure: 2005–2010

As time went on, security researchers started to think that they could make money from the threats that they discovered. During this time frame, researchers often contacted manufacturers asking to be paid for the details of the threat, or, alternatively, asking for expensive equipment they could use for further experimentation.

In most cases, networking equipment manufacturers simply didn't have a mechanism in place to deal with these types of requests. As a result, researchers didn't always disclose threats that they had discovered, so users sometimes faced threats that could have been mitigated quickly if they had been disclosed.

Threat disclosure: 2010–2013

During this time frame, vulnerability brokers became active. These were people or organizations who were figuring out how to monetize the information regarding the threat or vulnerability. Typically they offered to sell the information to the manufacturer with a limited time frame for the problem to be resolved.

Often, the offer to the manufacturer also included a notice that the threat would be disclosed at an upcoming security conference and that the major media outlets had been invited to attend the conference.

Threat disclosure now

What's really keeping network equipment manufacturers up at night now is the change in motives they've seen in threat disclosures since 2013. An exploit economy has developed where researchers are pursuing dangerous threats and vulnerabilities that they can profit from. The details of these issues are then sold on the black market to the highest bidder. The bidders may include criminal organizations, corporations, or even nation states looking to take advantage of important security holes. These vulnerabilities get "branded" and marketed by companies and individuals and the industry is impacted by them as an public event.

Clearly, the transition in threat disclosures from being intended to help protect the IT community to a situation where the intent may be to cause as much damage as possible is quite disturbing. This trend makes it ever-more important that you can trust your IT business partners.

Understanding What You'll Encounter

Threats come in many forms. Pretty much everyone has heard of the attacks on large major brand retail and insurance companies where the attackers were looking to steal personal data and possibly credit card numbers. Attacks like those on a major entertainment company are a bit harder to categorize because it appears that there may have been a mix of political, economic, and social motivations at play.

In addition to attacks on a single organization, many other types of threats also exist. For example, recent news stories have made people aware of vulnerabilities like Heartbleed, Poodle, bash, and Ghost. These types of exploits aren't aimed at a specific company or organization, but rather, they're aimed at third-party software that's commonly used throughout the

Internet. Often these vulnerabilities are intended to steal personal information including usernames, passwords, and credit card numbers.

A technical look at attacks

In addition to the named attacks you might hear about in the popular media, you've probably heard IT experts mention specific types of attacks. Here's a brief and somewhat technical look at what they're talking about:

- **SQL injection**: This type of attack occurs when untrusted data is sent to a computer as part of a command or query. The attacker's hostile data can trick the computer into executing unintended commands or accessing unauthorized data. This can bypass security checks, modify the back-end database, and possibly enable execution of system commands. SQL injection has become a common issue with database-driven websites.
- **Buffer overflow:** This condition exists when a program attempts to put more data in a memory buffer than it can hold, or when a program attempts to put data in a memory area outside of the boundaries of a buffer. Buffer overflows enable attackers to run unauthorized commands on your systems.
- **Cross-site scripting (XSS):** This type of attack enables attackers to essentially spoof the client into believing that content is being delivered from a trusted source, such as a webpage that's considered safe. This vulnerability may be used by attackers to bypass access controls. Their effect may range from a petty nuisance to a significant security risk. Using this vulnerability, attackers can inject malicious scripts into web pages, gain elevated access-privileges to sensitive page content, session cookies, and a variety of other information maintained by the browser on behalf of the user.
- **Distributed denial of service (DDoS):** This type of attack is one in which a large number of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service from the system to legitimate users. A computer under the control of an intruder is known as a zombie or bot. A group of co-opted computers is known as a botnet or a zombie army.

Chapter 4

Understanding Vendor Policies and Processes That Build Trust

In This Chapter

- ▶ Understanding why customer data protection must be a top priority
- ▶ Building the right foundations to secure your infrastructure
- ▶ Applying the necessary disciplines
- ▶ Understanding the necessary policies
- ▶ Considering the processes

Trust is a very important element in choosing any type of vendor, and in today's world, it's pretty clear that your organization's future may depend on finding partners that are trustworthy. Especially in modern networking technology, the policies and processes that a vendor uses make a huge difference in building trust.

This chapter looks at specific policies and processes that are important to consider as you evaluate different vendors.

Protecting Customer Data

REMEMBER

An important consideration in earning trust should be the way a vendor deals with customer data protection. The protection of customer data shouldn't be an afterthought but rather a high priority for the vendor.

A vendor can take a number of steps to make customer data protection important throughout its organization. Some of these include:

- **Ongoing awareness campaigns:** The employees at the vendor are a critical first line of defense in maintaining customer data protection. You want a vendor who makes sure that its employees are constantly aware of the need to protect customer data. This is a part of the overall security awareness and behavior employees need to apply to their roles.
- **Mandatory data protection training:** In addition to understanding the importance of maintaining customer data protection, the vendor's employees should also receive ongoing training so that they know how to properly apply the best practices that adhere to established policies.
- **Understand and communicate the value of customer data:** The entire organization must be made aware that customer data is as valuable as any physical assets. An organization should protect customer data as if it were its own data.
- **Taking proactive measures:** When a data loss happens or the opportunity arises to prevent a potential data loss, you want a vendor who will immediately address the situation rather than waiting for you to request a resolution. One of the key steps a trustworthy IT business partner needs to take is to implement an incident management process to identify any potential or actual customer data loss (or data loss events) in order to facilitate the most appropriate response.
- **Acknowledging problems:** No one is perfect, so mistakes will happen. Vendors need to admit their mistakes and proactively work to correct them as quickly as possible.

Making Sure There's a Solid Infrastructure Foundation

In many ways, building a trusted solution is like building a house. You need to start with a strong foundation and make sure that you include the proper elements.

For trustworthy infrastructure solutions, some of the proper elements a vendor must incorporate within its supply chain and development environment include:

- **Physical practices:** These include the various physical aspects of security, such as camera monitoring, security checkpoints, locking devices, alarms, and electronic access control to ensure that none of the components or finished products are tampered with or otherwise compromised. For example, you wouldn't want a network router that had third-party malware or spyware installed. Vendors need to protect products at all points in the supply chain to ensure high levels of security.
- **Logical processes:** Vendors need to apply systematic, repeatable, and auditable security processes that target security risks. They should ensure that all data is transmitted securely using modern encryption technologies. To prevent counterfeiting, they need to validate adherence to scrap-handling processes, produce the proper certifications of production, and make sure that any excess counterfeit protection labeling is destroyed to prevent inappropriate use.
- **Technology innovation:** Products should be designed so that they have anticounterfeiting measures incorporated to disable or quickly identify unauthorized components or software. These measures should be robust enough to prevent any malware or spyware from compromising your systems and data.

Looking for the Right Disciplines

A vendor can apply a number of supply chain security disciplines to gain and maintain your trust. For example, it's pretty obvious that you don't want network products that contain backdoors allowing unauthorized access, so you'll want a vendor that has a strict policy prohibiting the inclusion of such things in any devices.

A few other important disciplines you'll want to look for include:

- **Information exchange and access control:** Make sure that the vendor has a solid policy controlling what information is shared, the format of any shared information, the secure platform for sharing, and who should have access to that information.

- **Physical plant security**: Vendors need good processes to control access so that products can't be tampered with during manufacturing or distribution.
- **Personnel security:** Vendors need to be sure that employees are screened before they're hired and that they're fully aware of company policies such as those that pertain to customer data protection.

Of course, vendors also need to make sure that these and other important security disciplines are applied consistently across their supply chain. A trustworthy vendor will no doubt be happy to provide you with additional details about further steps that they take to ensure secure design, manufacturing, and distribution.

Looking for the Right Policies

Companies establish policies to ensure that people act consistently across the organization. If everyone follows the same policy, customers and vendors know what to expect.

There are certain types of policies that you want to look for in an IT business partner:

- **Transparency and open communications:** It's vital that your IT business partner isn't hiding an agenda that might be detrimental to your business model. You need a vendor who is open and transparent about its relationships.
- **Strong code of business conduct:** You need a vendor that establishes policies for all employees to make sure that they stand up to the highest business standards. The code of business conduct should reinforce the need for transparency, accountability, and leadership to protect products, data, the company, and customers.
- **International industry collaboration:** IT vendors must face up to the fact that new threats appear daily. By collaborating with other major players in the industry and

helping create product security standards, trustworthy vendors can be at the forefront of security and data protection, rather than simply reacting to emerging threats after the fact.

- **Ongoing security awareness:** Securing every process, policy, and technology requires security awareness in everyone. Understanding the vulnerabilities and threats specific to your job, be it software development, finance, sales, service, manufacturing, or any of the other positions needed to support the vendor's overall business, is fundamental to providing trustworthy solutions. This awareness comes with training, acknowledgement of problems and their solutions, and rewarding doing the right thing.

Security awareness training should be mandated across the trustworthy IT business partner's organization. All of these processes and policies must be kept top-of-mind in each employee along with a basic understanding of the threats and available mitigations. Keeping the information fresh and relevant requires a program that educates in easy-to-consume amounts, builds on previous knowledge, applies the new information in its current work assignment, and rewards individuals who continue to strengthen their knowledge and application within their assignments.

Depending on location, all networking equipment needs to meet certain defined standards. For example, equipment would have to be in compliance with prevailing electrical codes in order to be used legally. Likewise, there may be governmental requirements calling for the equipment to meet minimum security standards. You want a vendor who takes the lead in going well beyond any minimum requirements, if for no better reason than those standards typically lag behind emerging threats.

Looking for the Right Processes

It's great to have good policies in place, but you also need to implement the proper processes that make things happen. You might say that policies define what should happen and processes bring those policies to life.

One of the first processes that a trustworthy business partner needs is to implement a security-minded culture throughout the organization. In other words, product and data security must be maintained from the time that a solution is first designed all the way through to when that solution is delivered to customers.

Next, it's important that solutions obtain standards-based, multinational-security certifications. This is only possible when products are properly designed to meet the requirements of those certifications and also pass through the necessary security checkpoints along the way.

TIP

Look for solutions that have security embedded into their architecture rather than something that's added on later. Quite simply, you need to trust the entire solution, not just what someone might tack on top.

A real-world process example

Cisco's Product Security Incident Response Team (PSIRT) provides a real-world example of the type of process a trustworthy business partner might implement. This group is a special team within Cisco that was established specifically to respond to security incidents. Operating globally, the team manages the receipt, investigation, and public reporting of security vulnerability information relating to Cisco products and networks.

When PSIRT receives a report of a potential security problem, it investigates both the severity and scope of the issue. If the report turns out to be applicable, the team works with the appropriate people to try and find the proper solution. When they've resolved the problem, the solution is made available for distribution and all potentially affected customers are notified simultaneously.

To provide an additional layer of protection to customers, Cisco signs all PSIRT security advisories using public-key encryption. This extra step helps to protect against bogus security advisories that might be intended to fool customers into applying malware disguised as an actual Cisco security fix.

Chapter 5

Building Trustworthy Infrastructures

In This Chapter

- Understanding the changing nature of threats
- Building secure foundations
- Including the proper technology
- Making sure your systems are healthy
- Taking it to the supply chain
- Understanding the development life cycle
- Providing visibility

With today's need for instant communications and the broadly expanding range of cyberthreats, your business needs constant protection, starting with the best possible infrastructure components. You can't count on being lucky in regard to protecting your organization's assets and customer data.

This chapter provides a look at some of the steps a trustworthy IT partner should take in order to deliver the most trustworthy infrastructure it can.

Understanding How Threats Are Evolving

Today's cyberthreats aren't the same as yesterday's threats. Just as technology races forward and becomes more sophisticated all the time, attackers are constantly adapting their tactics to find new ways to breach security barriers.

It's no longer enough to throw up a fence at your perimeter and assume that you've done enough to stop the bad guys. Sophisticated attacks like Heartbleed have shown that danger can pop up anywhere in your systems. As a result, you need protection that goes well beyond simply stopping an email virus or a piece of malware posing as a free game download.

Making Sure You Have a Secure Foundation

There are best practices to providing the most secure foundations possible. These steps include:

- S**upply chain:** Security technology and practices should be deployed throughout the supply chain to assure authenticity. In addition, steps need to be taken to make sure no substitutions occur anywhere along the way.
- **Consistent blueprint:** Security should be a top priority during the entire product development process rather than something that's added on later.
- **Anchor of trust:** To secure a product, there must be a secured hardware or software component that is attestable and accessible but not changeable. This foundation is necessary if you want security by default to be possible in your infrastructure.

But even these steps aren't enough to provide the best possible protection. Further moves include:

- **Verifying authenticity at runtime:** Products incorporate technology to verify authenticity at runtime:
    - **Protected boot code:** The very first section of code that is executed is protected from changes, thus ensuring hardware integrity and key authenticity
    - **Randomized code base at run time**: Mitigate attacks on known software vulnerabilities

  - **Secure identity:** Provides a verifiable and unique identity that can't be tampered with to prove the product is genuine
  - **Secure cryptography base:** Provides a secure base so certificates can be validated
  - **Secure storage:** A protected memory area that protects keys and identity
- **Secure boot:** Ensures that only authentic software can boot up on a platform and prevents tampering with that software.
- **Next-generation encryption:** Makes sure that your data is protected with stronger, more efficient encryption using up-to-date protocols and identity validation.
- **Trusted local identities:** Uses enrollment, authentication, and certificate management to provide identity protection.

TECHNICAL STUFF

The technology controls the boot process by making sure that the very first code that can be executed can't be changed. This first section of executable code ensures both hardware integrity and key authenticity at device power up before the rest of the secure boot process can continue. As a result, only authentic software can boot. This technology performs the necessary tests while still allowing for validated updates of the operating system software.

Making Sure the Right Technologies Are in Place

Finally, trustworthy solutions need to have modern and sustainable technologies incorporated in order to deal with the latest threats. This section looks at a few of them.

Hardware security

Servers and network devices, such as routers that are actually specialized computers, need to boot and run a set of instructions. Those instructions tell the unit how to do things such as running an application or directing the flow of traffic on your network. You wouldn't want those instructions to be corrupted because then your data security might face serious risk.

One of the most effective ways to protect those infrastructure devices is to use technology that prevents unauthorized code from running on them. For example, Cisco uses something they call Secure Boot to verify that only authorized code can be run. In effect, this technology is designed to verify that Cisco has signed the code with the proper certificate before the device will actually execute that code. This means that it has secure development life cycle processes and policies to strengthen product integrity.

Strong encryption

With the openness of the Internet, it's quite easy for organizations to intercept and eavesdrop on data that isn't intended for them. One of the most common defenses against this sort of eavesdropping has been encryption. The problem is that many existing encryption algorithms aren't very strong, making it fairly easy for criminals or government spies to tap into encrypted data streams.

Work with a partner that not only provides the latest in encryption but also makes it easier to activate. Secure management of the encryption keys makes it easy to establish secure communications and to refresh or revolve keys. This capability allows teams managing today's BYOD as well as tomorrow's Internet of Things (IoT) environments a way to start devices securely — by default.

Enrollment over Secure Transport (EST) is a standard (IETF RFC 7030) to securely manage the identities based on certificates needed for RSA and Elliptical Curve Cryptography (ECC) encryption. Using either a secure identity from a device or username/password from a user, this method works with a registration authority (RA) connected to the certificate authority (CA) to authenticate the device attaching to the network and then send secure local identities (key certificates) to the device. EST can be used to securely establish, renew, and revoke keys to continuously keep your infrastructure and end points protected.

Certifications

Certifications provide a means of verifying that solutions meet specific minimum standards for a specific industry or government.

International certifications like Common Criteria provide a way for you to globally compare the protection profile of similar infrastructure devices. The supply chain should adhere to the guidance offered in ISO/IEC 27036 that addresses the evaluation and treatment of information security risks involved in the acquisition of goods and services from suppliers. A trustworthy partner's products should be designed with these baseline requirements.

Certifications are a moving target. Government agencies often require that networking solutions have certain certifications, but generally such requirements lag well behind the current state of the industry. It's important to have a trustworthy IT business partner who takes an active role in helping shape new standards rather than simply meeting the requirements of existing ones. The bad guys aren't standing still, and neither should you.

Ensuring System Health

Making sure that your systems have a good foundation provides a secure baseline, but you also want to make certain that things continue to stay healthy and function properly. You need ongoing, automatic inspections during operations to monitor the health of the devices.

Monitoring ensures run-time integrity by examining key vital signs for changes in such areas as:

- Device identity
- Secure boot status
- Hardware configuration
- Software configuration
- Files and processes

Applying Security across the Supply Chain

Creating a trustworthy infrastructure means that you have to have proper security across the entire supply chain. This means that products need to be designed securely from the very beginning and that same sort of thinking needs to apply throughout the life cycle.

For each product, the following steps need to have the proper security measures applied:

- Design/development
- Planning/ordering
- Sourcing
- Production
- Quality assurance test
- Product delivery
- Service/end of life (EOL)

Because components may be sourced from a number of vendors, it's important to make sure that each of them participates fully in these security processes. Applying proper security across the entire supply chain involves:

- Secure inventory locations
- Physical plant security
- Protection of high-value intellectual property
- Limiting system access to key personnel who have been properly screened and vetted
- Customs and border protection collaboration to restrict importation of counterfeit product

WARNING!

Vendors put customers at risk when they don't take the necessary steps to properly apply security measures across the entire supply chain. For example, counterfeit products typically lack a number of important security features because the counterfeiters are more interested in making the cheapest knockoffs possible and this means taking as many shortcuts as possible.

Considering a Secure Development Life Cycle

Trustworthy products need to be designed, implemented, and rigorously tested throughout their development life cycles. This is an ongoing process that works to eliminate as many potential problems as possible as early as possible in the development life cycle, while also addressing issues that become evident later through further types of tests.

The ISO (International Organization for Standardization) is a nongovernmental organization based in Switzerland that has members in 163 countries. The ISO publishes international standards such as ISO 27034, which defines a secure development approach that applies broadly across IT and networking application development and deployment. The vendor's secure development life cycle (SDL) should conform to ISO 27034 to provide a repeatable and measurable process designed to mitigate the risk of vulnerabilities and increase product resiliency.

Product development life cycles may vary somewhat depending on the manufacturer, but most trustworthy vendors likely follow a path fairly similar to the Cisco Secure Development Lifecycle (CSDL). The following sections review the specific stages of CSDL.

Although the secure development life cycle is presented as a set of six steps, in reality, it's an ongoing process that continues during a product's life cycle — it follows a waterfall development methodology or an agile development methodology. Each of the steps is repeated as many times as is necessary to discover both known and newly emerging security issues that might compromise a product or data protection. Whenever a fix or an update is proposed or created, it's important to verify the fix or update functions as expected and doesn't introduce any new security problems.

Product security requirements

To begin the secure development life cycle process, you first need to establish baseline security requirements. These requirements help ensure consistency.

TECHNICAL STUFF

Product security baselines are built over time from multiple inputs: previous product attack mitigations, industry reports on specific types of vulnerabilities, third party and open-source reported vulnerabilities, certification requirements, academic and internal research, and strong coding practices. To maintain the strongest protection, these requirements must be kept up to date and selectively applied to products based on those products' specific functions and uses in the market.

As a part of this stage of the process, an analysis examines the proposed product looking for any gaps in security that might exist. For example, boot and system integrity need to be verified to ensure that there are no holes that can be exploited.

Third-party software fundamentals

Next, the effects of any third-party software solutions on the overall system need to be considered. This includes performing an analysis of the software, verifying that there are no hidden backdoors, and addressing all known vulnerabilities.

The vendor must also include a plan for managing any third-party security alerts and contracting the appropriate parties to ensure there will be support for any critical security fixes. Obviously, the vendor must have a planned response in place to address any third-party security issues.

Threat modeling

A secure design must include a process to identify and assess risk, as well as to correct any security problems that might pop up during feature development. This means that development engineers must consider how each feature can be attacked and how best to deal with any such attacks.

REMEMBER

Threat modeling is not a one-time event, but rather it's a way of thinking about security for every feature throughout a product's life cycle.

Secure coding

All of the software in a product needs tamper protection to ensure that it won't be compromised. Cisco, for example, uses methods that can verify that its software hasn't been modified in an unauthorized manner.

Using libraries that have been well vetted is one method to avoid vulnerabilities in code. These code libraries are verified to ensure that they're safe and don't contain security holes. Code needs to perform proper input validation. Validation of this includes secure code reviews, checklists, and inspection.

Secure coding also includes the insertion of address space layout randomization (ASLR) and other boot time defenses that reorganize the address space to prevent attackers from reliably knowing the address of any code or data, preventing buffer overflow attacks.

Static analysis

Static analysis finds bugs by searching for common programming mistakes — some of which might be leveraged by hackers to compromise a system's availability or integrity. Static analysis of all code looks for particular types of vulnerabilities such as memory allocation issues, cross procedural dependencies, dead code, uninitialized variables, string validation, infinite loops, return code validation errors, integer overflow, and buffer overflows. This analysis is part of an ongoing process — the goal is to improve performance by finding more actual and important bugs while producing fewer false positives.

Buffer overflows are a commonly exploited error that can lead to allowing malicious code to run. Effectively, a buffer overflow means that something can be written to memory addresses inappropriately. Buffer overflows can be used to cause programs to crash, to output incorrect results, or even to execute malicious code, and are considered a very serious security and data protection concern. Computer code needs to be very carefully examined to make sure that it is protected from buffer overflows, especially because a number of important computer programming languages such as C and C++ contain no built-in protection against these exploits.

Vulnerability testing

Even the most securely designed and coded product needs to undergo extensive vulnerability testing to determine how it will withstand common attacks. Testing includes verifying proper responses to commonly used Internet protocols, resilience under flooding, and unexpected input (fuzzing) conditions. This type of testing allows the vendor to know how a product will withstand abuse, and to verify input validation is designed and implemented properly before releasing it.

In addition to checking hardware responses, vulnerability testing also seeks to verify the security of any software applications used by the product.

Providing Visibility and Control

Historically, it's taken far longer to detect and respond to system attacks than is comfortable. By some estimates, the vast majority of data theft and system damage occurs within hours, or at the most, a few days, of the original system intrusion.

Obviously, the sooner you can detect unauthorized changes in your systems, the better chance you have of protecting sensitive customer information. Your systems need to constantly monitor network devices looking for changes in their operating system, configuration modifications, new processes running on the systems, or unexpected login attempts. Once detected, your management systems need to evaluate these types of alerts and immediately notify system administrators when something suspicious is happening.

Chapter 6

Seeing What's Next

In This Chapter

- Seeing where we are
- Looking at the challenges
- Understanding where we're going

The world of protecting IT infrastructures presents a constantly changing landnormakscape. New technologies and new threats appear all the time, and you need to be aware of how these developments will affect your organization.

This chapter looks at the current state-of-the-art, and some emerging challenges, and provides a glimpse of what to expect in the near future.

Establishing Today's Baseline

One of the big changes between the way early computer networks functioned and the way networks are used today is that those early networks were largely stand-alone networks that served the needs of a single location or a single organization. Then organizations connected to the Internet, establishing a security parameter with firewalls and intrusion detection. Now everyone has computers, connecting to the Internet along with your company. Network and data security have become a much larger issue than they traditionally were.

A big part of IT infrastructure security is controlling access to your organization's resources. You want to make sure that people can't freely steal your data, or your customers' data, limit access to your business, or pretend to be representing your company. You need to protect your revenue, your intellectual property, your actual physical property, and your reputation.

Traditionally, it's been relatively safe to assume that people and devices were who they said they were. For example, if you wanted to run an application, you logged on. Or if you needed to take control and reconfigure a router, you simply entered the proper IP address, provided the correct username and password, and you were permitted to log in to make whatever changes you deemed appropriate.

But in the days of virtually universal Internet access, it's much harder to be certain that unauthorized users won't be able to gain access to your systems.

Looking at the New Challenges

Things have changed over the years and you now face many challenges that no one dreamed about in the early days of networking.

Are you who you say you are?

Establishing if people or devices are who they say they are requires the integrity of the person and/or device to be established. Although a username and password once provided safe access control, they're no longer sufficient protection.

Two-level authentication has long been a standard for authenticating a person. Devices with a predefined identity such as a Secure Unique Device Identity (SUDI), which is established at manufacturing, have a security key. That key can be used to establish a secure path during authentication as well as provide strong identity. This is a strong defense against man-in-the-middle attacks. Bringing the product integrity and secure communications together, you can see the start of security by default.

A man in the middle attack is a type of attack where someone is listening in and intercepting traffic somewhere between you and your intended recipient. The interloper may give you a response indicating that they're actually the intended recipients, and it can be very difficult or even close to impossible to know the difference.

Proving identities

Because both usernames and passwords are relatively insecure and man-in-the-middle attacks are technologically fairly easy to pull off, networking vendors have had to come up with far more secure ways to deal with these types of issues for both people and machines. One of the more recent ways is something called *attestation,* which basically means proving that you're indeed who you say you are — and that you're functioning properly.

TECHNICAL STUFF

Both users and devices can prove their identities using certificates that can be verified through a method called *public key encryption.* Basically, each device or user has two keys that are used to establish their identity. One of these keys is private and one is public. A mathematical algorithm creates the public and private keys as a pair. This pair of keys shares a unique quality. Anything encrypted by one key can only be decrypted by the other. That means if one key is kept private by you, and you publish the other, anyone can use your published key to encrypt a message only you can decrypt. You can use your private key to encrypt a message to someone else as proof you sent it (because your public key can be used to decrypt it).

Verifying the health of your devices

In addition to authenticating the identities of users and devices, you also need a means of verifying that someone hasn't modified the code inside your devices. You need to make sure that a router doesn't have malware installed and that its configuration hasn't been changed without your knowledge or permission.

TECHNICAL STUFF

Once again sophisticated mathematics come to the rescue. Computer code can be run through an algorithm that creates what is known as a *hash code*, which is a unique value that changes whenever any modification is made to the software. Your network control devices can maintain a database of the most recent hash codes generated by your routers and other network devices. When one of those remote devices is accessed, a two-step process first uses attestation to verify the identity of the device, and then the device is asked to supply its current hash code. If that hash code is different than the value stored in the database, you know that some unauthorized modification has been made and the device can't be trusted.

WARNING!

Although attestation and hashing provide fairly robust security, both suffer from a similar shortcoming. In both cases, network devices are verified either during their initial boot process or when they're first communicated with over your network. This means that although you can tell that the device was unmodified in the beginning, it's still possible that unauthorized changes could have been made sometime after those first verification steps. In the case of devices that might run for extremely long periods of time without interruption, such as remote sensors, you could be dealing with corrupted data or device modifications and not know it. That's why companies like Cisco are currently developing solutions to verify the run-time integrity of various networked devices.

Along with strengthening attestation throughout the life of a device, knowing the health of the products and therefore your infrastructure becomes important input, along with your security products protecting data and users, into your overall security posture. Having all the status information gathered securely allows you to see where gaps may be in your defense of your company.

Achieving and maintaining security is hard

The notion of *secure by default* implies that the vendor has taken steps to design a product that boots securely and then continues to operate securely, protecting itself and customer data passing through it. It also enables an advanced concept in networking called *autonomic networking*. In this model, the network handles problems of provisioning and configuring new gear, raising alerts on infected gear, rerouting data when a device goes down, and other functions. The savings to the customer are obvious, but these savings can only be achieved if the devices can be trusted.

Autonomic networking is a way to manage networks where the dependencies on human operators and network management systems are drastically reduced. Everyone wants a much simpler interface — and what is happening in the network needs to be much more predictable. By putting the intelligence required to run the network into the nodes themselves, self-configuring routers, switches, and other devices will drastically simplify network management — to the point where it should be possible to manage and secure even a very large network using a smartphone. An autonomic network needs central input for consistent network policy as established by SDN (software defined networking). A centrally controlled network, on the other hand, needs embedded intelligence in order to reroute quickly enough around a link failure. Together, security by default will protect the infrastructure as it morphs to meet your business needs.

Looking to the Future

The way people use computing devices is changing rapidly. One example of this is how quickly the various services have been moving to the cloud. Just a few years ago, most companies had their own in-house data center that supplied the bulk of the organization's needs for computing services. Now, it's far more common for those services to be hosted in the cloud. It's likely that this trend will accelerate in the near future, so you need to look for a trusted partner who understands this new world. Trustworthy cloud moves the functions of product integrity, secure communications, attestation, and control into the virtual world.

Virtualization creates easy-to-move applications and their workloads, and cloud computing brings new efficiencies. However this rapid change means that you need to apply a whole new mindset to security and data security issues, asking questions such as "Is my application and data running on a healthy platform?" or "Is my data compliant with the physical location requirements my industry or government requires?"

An even bigger change is about to rock your world if it hasn't already. The Internet of Things (IoT) is bringing a whole new dimension to networks everywhere. Very soon, all sorts of devices with many different types of sensors will be connecting to networks and sharing huge amounts of new data. People often cite the example of smart refrigerators that will supposedly tell you when your carton of milk or package of eggs is about to go bad. But the IoT is about a lot more than smart appliances in people's homes.

A real-world example of the IoT relates to physical infrastructure such as underground pipelines or the power grid. Imagine, for example, an underground gas pipeline with Internet-connected pressure sensors that can be used to detect leaks or to control the flow of gas through the pipeline. Obviously, allowing the bad guys to gain access to those sensors and tamper with the pipeline would be a very bad outcome. Likewise, imagine if a rogue nation state were able to access the power grid controls and shut down the country's power. The price point, size, weight, and power of IoT brings another level of innovation to security by default for trustworthy IoT. Having the capability to establish visibility and control while allowing the many systems that support modern existence to continue their mission is mandatory for IoT.

WARNING!

Although the IoT offers many wonderful opportunities for automating things that were either difficult or impossible to automate in the past, it's also clear that many new risks and dangers are also emerging. Once again, you need a trusted network systems business partner who is working on making sure that the IoT is as efficient, safe, and secure as possible.

Chapter 7

Ten Things to Look For in a Trustworthy IT Business Partner

In This Chapter

- Checklist of trustworthy IT business partner characteristics

This chapter brings it all together to tell you the ten most important characteristics you want in a trustworthy business partner.

Being Transparent

When looking for a trustworthy business partner, transparency in its processes, policies, and technology should be a key consideration. This continuous transparency will help you understand how the company does business and provide you with a better idea of whether it will be a good fit with the needs of your organization.

TIP

You want to make sure that a vendor's transparency includes providing proof of its security posture as well as known vulnerabilities so that you can make an accurate evaluation of the fit with your risk posture. For example, you'll probably want a vendor who places top priority on safeguarding customer data and lets you know when information is at risk.

Being Accountable

A trustworthy business partner must be accountable for its products and services throughout the life cycle, providing updates and mitigations to new threats as well as being diligent to solve problems as they arise.

It must also be responsible, reliable, and responsive to the on-going attacks against its own company as well as you and its other customers. This will help ensure the business continuity that's necessary for a long-term relationship.

REMEMBER

A trustworthy business partner must be diligent in helping you secure your overall business with the breadth of trustworthy products and the depth of security products and services.

Being Security Aware

A trustworthy business partner should ensure that everyone in the solution life cycle is trustworthy and security aware. This includes the development, sales, service, financing, supply chain, and partners in the vendor's ecosystem. On-going training and awareness programs help keep this responsibility top of mind.

Securing the Entire Supply Chain

It's vital to manage the longer, more complex supply chain common in today's manufacturing processes with strong security processes, policies, and technologies. Supply chain security must extend from the concept of the solution and/or product through the development, manufacturing, delivery, service, and to the end-of-life/disposal processes, policies, and technologies to allow for the global sources through the life cycle.

TIP

You want a vendor that knows how to assess risks in the supply chain and understands the importance of protecting critical assets that impact the security of supply chain.

Keeping Current on Threats

A trustworthy IT business partner must be intimately involved in most current infrastructure environments like the cloud and the Internet of Things to understand both the threats and the mitigations needed to secure these environments.

Another good measure of a trustworthy business partner is a willingness to fund cybersecurity research and industry awareness as well as maintain a strong proactive understanding of the attackers and attacks on the infrastructure. Remember, threats are constantly evolving, so protection must evolve as well.

TIP

Take an approach that encompasses other industry players because few threats are so specific that devices from only one vendor are at risk of compromise. When a number of important organizations cooperate in looking for vulnerabilities, the chances of finding the problems and their solutions greatly increase.

Protecting All Data

A trustworthy business partner must protect customer and company data throughout the solution life cycle with transparency on technology, processes, and policy and accountability when mistakes happen. Not only is this an ongoing commitment, but it's also one that requires that a vendor have established processes to deal with any contingency.

REMEMBER

Taking responsibility when mistakes happen rather than trying to shift the blame elsewhere means that problems can be quickly resolved before damage becomes severe. You need a vendor who will acknowledge issues and work with you to find solutions.

Practicing a Secure Development Life Cycle

It's hard to overemphasize the importance of a secure development life cycle. This process injects security-centric technology and procedures into every step of the design and engineering phases of product and service creation and development.

Providing Security by Default

The best, most powerful security features are useless if they aren't implemented and used. You want solutions that provide secure hardware and software as foundational features, built into the product from the beginning and supporting security by default.

Considering Differing Needs

It's important to remember that situations may vary greatly. You need a vendor who will meet the combined security and assurance standards and certifications needed by the different markets.

Being Consistent

Finally, a business partner must continuously strive to be trustworthy as trust must be earned every day. In other words, trust isn't simply a slogan but must be an ongoing part of the vendor's DNA.

With today's threats, you need to choose business partners you can trust

Cyberthreats and attacks make life difficult for all organizations. You need to know how to choose the right IT business partners who will help you survive without becoming the next sensational headline news story.

- ***The bad guys are out there* — choose the right IT business partner that will watch your back**
- ***Policies matter* — see what vendor policies and processes can do to help protect your interests**
- ***Threats are evolving* — you want an IT business partner you can trust to be ready to address the future**

Open the book and find:

- **What you need to protect**
- **How vendors can help look after your interests**
- **Ways to secure your infrastructure**
- **Why trustworthiness should be built into your hardware and software**
- **How to evaluate potential business partners**

Brian Underdahl is the author of over 135 books including many *For Dummies* titles. He's been a part of the tech industry for many years and enjoys making technology understandable.

FOR DUMMIES®
A Wiley Brand

ISBN 978-1-119-10214-4
Not for resale