Securing the Extended Enterprise

TABLE OF CONTENTS

The Extended Enterprise ................................................................. 2
Security Challenges of the Extended Enterprise ................................ 3
  The Perimeter Has Vanished ......................................................... 3
  Threats Have Changed ............................................................... 4
  Data Is Everywhere ................................................................. 4
  Risk and Compliance .............................................................. 4
A New Approach Is Required ......................................................... 5
  Think Wider ............................................................................. 5
  Think Deeper .......................................................................... 5
  Think Smarter ......................................................................... 5
Securing the Infrastructure .............................................................. 6
  Aligning Policies, Processes, and Procedures ................................. 6
  Aligning Your Security Architecture ........................................... 6
  Filling Security Technology Gaps ............................................... 6
  Ongoing Monitoring and Management ........................................ 7
Securing the Information ................................................................. 7
  Know Your Data and Where Your Data Sits .................................. 7
  Protecting Your Data .................................................................. 8
  Protecting Your Applications and Users ....................................... 8
  Detecting Data Breaches ............................................................ 8
  Responding to a Data Breach ..................................................... 8
Information Security Governance, Risk, and Compliance ..................... 9
  Risk-based Security Decisions Backed by the Business ................... 9
  Assessing the Risk .................................................................... 9
  Addressing Third-party Risk ...................................................... 9
  Addressing Security Compliance Requirements ........................... 10
Summary ....................................................................................... 10
The Extended Enterprise

For decades, technologists in the security industry believed that the best strategy to protect an organization was to build a strong wall around it. This so-called “perimeter model” assumed that the virtual boundaries of an organization were very similar to the physical boundaries. In the early days of the Internet, this assumption was essentially accurate. Connectivity between an organization and the outside world was limited and easily identified. “Keeping the bad guys out” was the motto, prompting the development of a broad range of network-focused security products.

Today’s reality is completely different. Modern business requires that companies expand their traditional perimeter to allow partners, suppliers, auditors, manufacturers, remote offices, and remote employees to access applications and information. We call this new business model the extended enterprise.

Securing the Extended Enterprise

The extended enterprise enables businesses and governments to:

- Improve customer/citizen service
- Bring services to market quicker
- Make better business decisions
- Increase productivity of mobile workforce
Security Challenges of the Extended Enterprise

Now that organizations have opened up their business applications and data to partners, suppliers, internal divisions, and remote workforce, they need to revisit their existing security practices. Just relying on the old perimeter security practices is not sufficient, as those practices do not address many of the new security challenges that come with the extended enterprise.

The Perimeter Has Vanished

A first challenge relates to the existing security infrastructure and how it needs to be changed to span the complete extended enterprise. In the old ‘perimeter’ paradigm, we started from the assumption that we could split our world in two: the trusted inside and the untrusted outside. Everything sitting within the walls of our organization, including users, data, and applications, was supposed to be under our control and didn’t require a lot of attention from a security perspective. Everything outside of our organization was beyond our control, so it could not be trusted. The solution was to build a big security wall around that perimeter focused on inspecting incoming network traffic.

Unfortunately, the perimeter as we defined it in the past no longer exists. The difference between what we called the inside and the outside has faded. Remote offices are connected to our headquarters, contractors walk in and out of our offices all the time, our employees now have mobile devices allowing them to connect from anywhere anytime, suppliers are connected to our inventory system in real-time, business partners access our customer relationship management (CRM) system, and vendors have remote dial-in access to maintain our IT systems. The perimeter has been pushed out to endpoints and to third parties. So is it fair to assume that our big security gateways still adequately protect our extended enterprise?

Today, your security program is only as strong as your least reliable business unit or business partner in the extended enterprise chain. Organizations rely on partners to deliver vital services, yet most don’t recognize the information security risk that those business partners or suppliers pose. In a recent Verizon Business Security Solutions survey, 32 percent of participants reported an incident through a business partner. Furthermore, the survey showed a clear correlation between the number and level of partner-related business activities and the likelihood of security incidents.

Partner-related business activities that increase likelihood of security incident.

© 2007 Cybertrust Research Survey.
Threats Have Changed

In parallel to this paradigm shift away from the perimeter model, we have also seen the threat landscape change significantly. Mass attacks are diminishing in number, while covert targeted attacks are clearly on the rise. The objective of these attacks is to breach the target without triggering any alarms or awareness. In 2008, the notion that a breach would occur in which the criminal was not attempting to compromise sensitive data is unheard of. The days of “innocent network exploration” are over—all network intrusion cases today should be considered malicious in nature. Hackers—which now include organized crime—break into systems with the outright intention of compromising sensitive data and converting it into cash.

The hundreds of forensic investigations performed by Verizon Business Security Solutions in 2007 confirmed this: approximately 75 percent of the companies that went through an investigation learned of the breach through an allegation after the fact. So the fact that there are fewer mass attacks to read about in the papers doesn’t necessarily mean organizations are more secure today.

Data Is Everywhere

Another important challenge in this new virtual environment relates to business data and business applications. In the perimeter model, we assumed that critical business data was securely stored in a central corporate database, protected from the untrustworthy world. In the extended enterprise, business data no longer only resides in corporate databases, but also on desktops, laptops, USB memory sticks, PDAs, and other portable devices. Business data is also crossing the enterprise boundaries and is exchanged with business partners, suppliers, and whoever requires access to the data through web-based applications.

The numbers speak for themselves. Business data worldwide is expected to swell to 988 billion gigabytes by 2010, up from 161 billion gigabytes in 2006. An estimated 162+ million records were reported lost or stolen in 2007, more than triple the 49 million that went missing in 2006. Many of today’s mobile devices have a standard memory capacity of 80 megabytes, the equivalent of 6,000 Microsoft® Word documents, 720,000 e-mails, or 360,000 contact details. Understanding which data is critical to your business and protecting that data adequately is more important than ever.

Risk and Compliance

The last and probably most complex challenge is to fundamentally align security with business goals and strategy. In the extended enterprise, information technology and information security are expected to enable business in its own context. As a result, businesses are not interested in individual threats or vulnerabilities, but expect an end-to-end security blueprint. The questions important to business are, “Is our online banking application secure?” and “Is our supply chain system well protected?” Businesses also expect security decisions to be based on the intrinsic business risk, engendering the challenge to position security in a business context.

Aligning security with the business assumes that an organization is able to measure security and to address security compliance requirements. Only mature, consistent, and repetitive security practices enable the extended enterprise to measure its security posture. Creating the tools and processes that facilitate this measurement is essential to the success of security and compliance programs.
A New Approach Is Required

Addressing the various security challenges discussed earlier in this paper requires a new approach. Organizations have to reconsider the way they handle information security by thinking wider, deeper, and smarter.

Think Wider

Security controls must span the complete extended enterprise. Controls should penetrate towards the edges of the extended enterprise to securely conduct business with suppliers, business partners, and more. They should also suffuse widely within the organization to secure remote offices, endpoints, portable storage devices, and wireless access points.

Think Deeper

Historically, we have spent over 90 percent of our security technology budgets on technologies that secure the network layer. However everyone agrees that ultimately it is all about information security. How do we protect the business data, the applications that process this data, and the user access to that data? It is an imperative for security controls to span the entire information technology stack, including the network, data, applications, and users.

Think Smarter

For years, vendors of security technologies have trained us to respond instantly to individual threats and vulnerabilities. Sometimes that is needed; however, often it is a waste of resources. Instead, security decisions should be based on the nature of the risk, not on just threats or vulnerabilities. Security controls should view risk as the locus of the assessment calculation.

In the next three sections, we discuss how this wider, deeper, smarter approach can be implemented in an organization. Solutions are suggested to systematically address the security challenges of the extended enterprise at three different levels:

- **Securing the infrastructure:** making sure that your security infrastructure spans your complete extended enterprise and that it is monitored and managed effectively

- **Securing the information:** making sure that your security controls include the protection of the actual business information

- **Addressing information security governance, risk, and compliance:** making sure that your organizations is able to measure against risk and address security compliance requirements
Securing the Infrastructure

This section addresses what organizations should do to align their existing security infrastructure and practices to effectively protect their extended enterprise.

Aligning Policies, Processes, and Procedures

It is a good security practice to review your organization’s security policies, processes, and procedures on a periodic basis. As will be discussed later in this paper, they should be aligned with your business risk, and should span the complete extended enterprise. Special attention should go to third parties such as business partners, suppliers, and vendors. Reality shows that the security policies and procedures of a lot of organizations do not take into account third parties. Yet the forensic investigations conducted by Verizon Business Security Solutions demonstrate that 65 percent of all breaches investigated in 2007 are “partial insider” jobs, meaning the source of the breach was found with a business partner, supplier, or vendor.

Let’s take a simple example. Does your organization have a policy that prohibits third parties that need to connect to your infrastructure from using shared support IDs across their customers? In a recent forensic investigation, Verizon Business Security Solutions came across a supplier that had its 40 support engineers use the same user ID/password combination across its entire customer base. Your organization surely does not allow such practice internally, so why would you allow a third party to conduct business insecurely?

Aligning Your Security Architecture

The next step in securing your extended enterprise is reviewing your current security infrastructure to make sure it correctly incorporates all parts of your extended enterprise. How has your organization segmented its network? What security technologies do you use to enforce secure remote access? How is endpoint security handled across your extended enterprise, including third-party endpoints that are beyond your control?

A security architecture review combined with a vulnerability assessment can help identify weak spots in your infrastructure and allow you to proactively address those before incidents occur. Let’s take another example. Does your organization allow third parties to connect to your network to access certain applications? If so, have you segmented those third-party connections from internal remote connections? Often, third parties are granted access to a large part of the network, rather than limiting their access to just those applications they need for business purposes.

Filling Security Technology Gaps

A gap analysis between your security policies—stating what you want to secure and to what extend—and your security architecture—showing what you actually do secure and to what extent—will show you where you may have to add security technologies. As an example, if you have a security policy that says that critical business applications have to be scanned for vulnerabilities and protected from the most commonly exploited application attacks, then your security infrastructure should incorporate application scanning and application firewall technologies.

Once gaps have been identified, appropriate security technologies need to be selected, deployed, and properly configured. If your organization lacks expert skills, you can work with a vendor-neutral security service provider to assist throughout this process. You may also consult ICSA Labs (http://www.icsalabs.com), one of the security industry’s central authorities for research, intelligence, and certification testing of products.
Ongoing Monitoring and Management

But technology alone is not the answer. The policies and procedures that govern security operations are just as important, as well as having the experts that are able to apply those policies and procedures and get the best out of the technologies in place. Day-to-day security operations remain a challenge. How do you correlate security logs and alerts across the organization to discover security incidents swiftly? How do you keep your security infrastructure up to date with the changing threat landscape? How do you keep up with and prioritize patching vulnerabilities? How do you handle and store security log data in view of audits?

Organizations choosing to run their security operations in-house need to invest equally in people, technology, and processes. On the people side, a security operations organization consists of various profiles including security analysts, security engineers, and an incident response team. Maintaining 24x7 coverage is challenging but has become a must. On the technology side, security event management (SEM) technology—which allows you to filter security events out of large amounts of logs and alerts—is an absolute must. When evaluating SEM technologies, do not just focus on their core correlation features, but look at the bigger picture. How difficult is it to build and maintain the SEM policy? How can the SEM interact with your ticketing system? Which actionable reports can be generated? And last but not least, make sure you have solid processes in place. Examples include change management, incident management, and problem management.

Given the cost and complexity involved with security operations, most organizations prefer to outsource the ongoing monitoring and management of their security infrastructure. Managed security service providers (MSSPs) typically serve hundreds of clients, and therefore can scale their organization, their technology, and their processes, allowing them to do the job better and more efficiently than an in-house security operations team. When selecting an MSSP, make sure you review the structure and size of their security operations organization, get a good understanding of how and how often both organizations will interact, and ask for sample reports and a demonstration of the portal they use to interact with you. Also keep in mind that only MSSPs with a sufficient size will be able to offer a good service around the clock. So ask for the number of clients they serve and where these clients are located. MSSPs with only a regional client base tend to serve you well during business hours, but may lack resources at nights or during weekends.

Securing the Information

Next, we discuss how to best approach the challenges faced by organizations—businesses and governments alike—when securing data, the flow of data, and the access to data.

Know Your Data and Where Your Data Sits

Data no longer sits in corporate databases alone and it flows in and out the enterprise, stored in remote databases. Furthermore it is sent to wireless and mobile devices where it may be stored or sent on again. Data privacy legislation, which varies by country, must be respected, and adds another layer of complexity to data access and management.

Most organizations are unsure of where their critical data sits within the organization. The reasons are common and varied—merger and acquisition activity, employee turnover, and spreadsheet data management often compound each other. Whatever the reason, businesses can lose track of their business information. In addition, organizations often deploy far too much security around the wrong data—spending time, dollars, and technologies on non-critical assets while leaving the truly sensitive data exposed.

All of that makes data classification more important than ever. You must have a good understanding of the data that is handled within your organization, the level of criticality associated with various types of data, and where that data resides. Data discovery technologies can be helpful in that respect. Once you know your data, you can start to put in
place security controls. Security controls should be aligned with the criticality level of the data, the risk associated with losing that data, and with security compliance requirements related to data.

Protecting Your Data

A first important step—which often is ignored—is awareness creation, making sure that the owners and users of the data understand what is expected from them when handling the data. Do certain types of data have to be encrypted at all times? Is storing certain types of data on mobile devices prohibited? What is the policy related to the use of mobile storage devices?

In a next phase, security technologies can be deployed to enforce the protection of data. Various technologies exist: encryption software, content monitoring and filtering (CMF) technologies, data loss prevention (DLP) technologies, enterprise rights management (ERM) solutions, and more. It is important to select technologies based on your objectives and that are aligned with the risks identified.

Protecting Your Applications and Users

Next to protecting the data itself, organizations should also protect the business applications and the users that access the data. Business applications with access to critical data should be scanned for vulnerabilities and, in some cases, protected by specific technologies such as application firewalls.

The identity of users must be managed carefully, and strong authentication of users using digital certificates or one-time passwords may become a requirement. Access management technologies that manage who is allowed to access what can be a cost-efficient alternative over user access controls embedded in applications.

Detecting Data Breaches

Once awareness has been created and security controls are in place, the hard part of vigilantly monitoring the infrastructure for potential incidents starts. As the forensic investigations conducted by Verizon Business Security Solutions have demonstrated, in the vast majority of cases, victims of a breach had not detected the breach until long after it occurred.

Around-the-clock monitoring of a security infrastructure to detect potential incidents is a complex task and can become very expensive when conducted fully in-house. Organizations should seriously consider outsourcing 24x7 monitoring tasks to an MSSP. A good MSSP has security experts available around the clock and is well equipped to perform these monitoring tasks better and more efficiently than an in-house security team could ever do.

Responding to a Data Breach

Once a serious security incident occurs—often including some form of data breach—an incident response and forensic analysis procedure should kick off, aimed at containing data loss, managing evidence, and strengthening defenses. Most organizations are not prepared for breaches. They lack pre-defined procedures, an understanding of what is required to maintain a chain of custody, and the expertise required to contain a breach. Organizations should develop an incident response (IR) program. Alternatively, they can proactively sign up with a provider of forensic services. Such a retainer agreement allows the provider to get to know your environment up front and can result in a quicker and better response in case of a breach.
Information Security Governance, Risk, and Compliance

At the end of the day, organizations want to be able to measure, report, and aggregate security information in order to make better risk-based decisions and to address security compliance requirements.

Risk-based Security Decisions Backed by the Business

For security success across an extended enterprise, there has to be a strong mandate to make it part of the executive management business plan. Business partnerships that understand this can effectively reach their security goals. Because security is now being woven into the fabric of the business plan, involvement at the top level of management is critical.

In the opposite direction, security organizations have to take security decisions based on risk, selecting those initiatives that deliver the most risk reduction to the business. Having a thorough understanding of the business risk therefore is the cornerstone of any information security program.

Assessing the Risk

A risk assessment, whether it is conducted in-house or by a security service provider, has to identify all areas of risk involved in the business, and quantifies each pocket of risk. Quantitative risk modeling (QRM) techniques can be helpful in this context.

The outcome of a good risk assessment is invaluable. It will basically guide you in making the right decisions. Should you invest in protecting the thousands of laptops out in the field, or should you invest in better protecting your central enterprise resource planning (ERP) system to which all of your suppliers are connected? Your risk assessment will tell.

Addressing Third-party Risk

The extended enterprise has allowed us to seamlessly integrate business processes between our own organization and that of our business partners and suppliers. Yet organizations tend to only consider their end of these business processes when it comes to security. The following graph—taken from a 2007 Verizon Business Security Solutions survey—shows that less than 25 percent of organizations assess the security aspects of doing business with third parties.

When does your organization assess the security of its business partners’ information systems?

- Never
- Prior to partnership
- During the partnership
- Both prior to and during
- Not sure
The same survey demonstrated that businesses that set a high priority on third-party security face about half the security incidents as businesses that do not. Survey respondents that leveraged a third-party security assessment program demonstrated a substantial reduction in the likelihood of security incidents. Security assessments can offer a reciprocal advantage to your business partners by documenting to others their due diligence in addressing third-party security issues. You should work with partners to review current security practices and their compliance with security standards.

Developing a third-party security program does not have to come with a lot of overhead. Some security service providers offer Security-as-a-Service programs that automate the entire third-party security assessment process by using a combination of self-assessment questionnaires and automated scans resulting in actionable compliance reports.

**Addressing Security Compliance Requirements**

Over the last few years, the number of regulations and industry mandates that come with specific security compliance requirements has increased. Initially, many organizations set up project teams for each regulation or mandate. Today, organizations look for more scalable and more cost-efficient ways to address their security compliance requirements.

The solution is to reach higher by benchmarking compliance requirements across multiple standards, as opposed to managing compliance regulation by regulation and propping up “compliance silos.” In other words, set the bar at a level where any compliance requirement can be met through a consistent compliance program.

There are many ways to set up a security and compliance program. Large organizations may consider purchasing governance, risk, and compliance (GRC) enterprise software. It allows you to consolidate information across your organization to then run various risk and compliance simulations and reports. GRC enterprise software has proven to be very valuable, but comes at a high cost in terms of both licenses and implementation resources.

An interesting alternative for many organizations is working with a service provider that offers security and compliance programs. Such programs can vary from self-service applications through fully managed programs. An automated assessment-based application may be the perfect solution if you need to comply with a concrete mandate such as the Payment Card Industry (PCI) Data Security Standard. If you want to build a true security program that can address multiple compliance requirements at the same time, a fully managed program may be more effective. When signing up for such program, the service provider will guide you throughout each program step—from an initial assessment up to periodic on-site audits—and provide advice on how to address issues that hinder meeting security compliance requirements.

**Summary**

The extended enterprise offers plenty of opportunities for businesses to grow and for governments to improve their services. At the same time, the extended enterprise comes with new security challenges. In order to effectively address these challenges, organizations must move beyond the constraints of historic approaches. The conventional perimeter model—building a security wall around the organization—no longer works.

A new approach is required. Organizations have to revisit the way they handle information security by thinking wider, deeper, and smarter. Wider—ensuring that security controls span the complete extended enterprise, including remote offices, mobile workers, business partners, suppliers, and vendors. Deeper—ensuring that security controls span the entire IT stack including the network, the data, the applications, and the users. Smarter—ensuring that security decisions are based on the level of risk reduction they bring to the business.
Putting the wider, deeper, smarter approach into practice can be done by systematically addressing the security challenges of the extended enterprise at three different levels:

- Securing the infrastructure
- Securing the information
- Addressing information security governance, risk, and compliance

Securing the infrastructure starts with aligning policies, processes, and procedures with your business risk across the extended enterprise. These policies should be reflected in the security infrastructure, and, in case of gaps, additional security technologies may need to be added. Ongoing monitoring and management of the security infrastructure has become a requirement. For many organizations, outsourcing these tasks has proven to be a cost-effective solution.

Securing the information starts with knowing and classifying your data to then deploy security controls to protect the data based on its level of criticality to the business. In addition to the data itself, business applications and users need to be protected. Both technologies and processes need to be in place to detect and respond to data breaches. Being prepared is the secret to success.

Addressing information security governance, risk, and compliance completes the process of securing your extended enterprise. Establishing a risk-based culture backed by the business and getting a good understanding of the risks across your organization are a prerequisite. A good security program will not only help manage risk, but will also provide a cost-efficient way to address the multiple security compliance requirements that your organization is faced with.

For more information, visit www.verizonbusiness.com.