WHITE PAPER

Market Pulse

An Inside-Out Approach to Enterprise Security

When burglars break into a home, they look for electronics, jewelry or cash – yet homeowners focus mostly on securing their doors and windows, not their valuables inside the house. This mindset permeates business as well. A CSO Market Pulse survey finds that two-thirds of security budgets are used to protect the network, with less than a third used to directly protect the data and intellectual property that reside inside the organization. It's clear from these results that most organizations are focusing an inordinate amount of attention on network vulnerabilities and neglecting their most valuable assets: applications and data.

It's not that securing the perimeter is a bad idea. The challenge is that for most enterprises, the network has become so large – encompassing multiple countries across the globe, outsourced data centers and, more recently, private and public clouds – that it's virtually impossible to secure the perimeter completely from cyber attacks and other external threats. Expect the trend to continue as more IT services are outsourced or moved to the cloud.

As our networks become even more complex and blurred, IT organizations have to transform their security strategy to keep up. Instead of only thinking about "doors" and network security, IT organizations need to refocus attention on their business's most strategic assets: the applications and data in the enterprise. Securing access to customer data, intellectual property and financial data at the source can save companies time and money.

For this reason, instead of focusing on more complex network security policy, IT organizations should focus on how users access applications and data. When criminals breach a network, they target weak user access controls as a means to acquiring valuable information assets.

By not aligning security budgets with their organization's most valuable assets – the information stored in databases, applications and servers – security teams are leaving the enterprise vulnerable to attacks from inside and attack vectors that bypass the perimeter. As such, there's a growing imperative for CSOs and CISOs to rebalance security resources to protect corporate information from the inside out.

A Rising Threat

Despite acute awareness of the importance of information security and compliance, the number of corporate data breaches continues to increase. Research by Verizon tracked 855 data breach incidents worldwide in 2011, accounting for 174 million compromised records – the second-highest total since Verizon began tracking such incidents in 2004.[1]

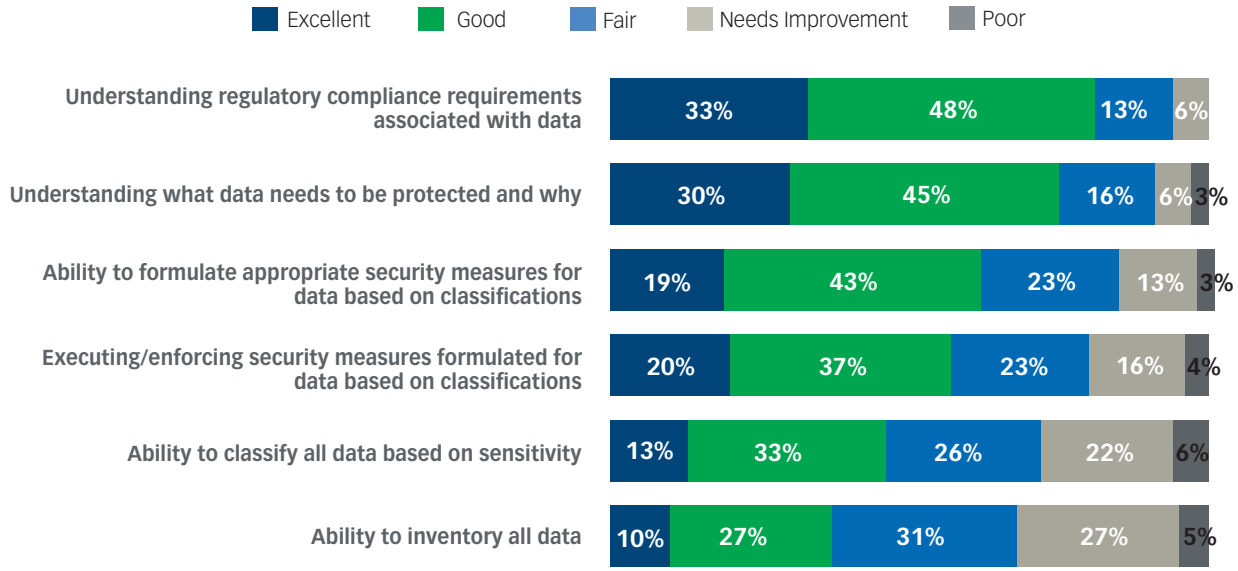
Ninety-eight percent of the attacks Verizon investigated came from external sources. More troubling, 96% of the attacks were deemed "not highly difficult," and 85% of the breaches took "weeks or more" to discover. That's more than enough time for cyber criminals to collect a business's crown jewels and do untold damage to its brand.

For more than half of the organizations in the CSO Market Pulse survey, the answer to rising threat levels is to spend more on security. But bigger budgets have not increased CSOs' confidence in delivering a highly secure enterprise. While 59% of respondents say their IT security budgets have increased during the past 12 months, only 23% say their organization has a superior strategy in place across all key aspects of data security.

"Much of the budget spent on IT security today is reactive," says Naresh Persaud, director of product marketing security

[1] "2012 Data Breach Investigations Report," Verizon, 2012 http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

Data Security Capabilities within Organizations



SOURCE: IDG RESEARCH SERVICES, NOVEMBER 2012

at Oracle. "When criminals break in, organizations focus on responding to the crime, but spend little attention on long-term strategic activity to protect the information assets and the databases."

Often, Persaud says, the most exploitable targets are humans, not machines. "It is far easier to exploit weaknesses in human behavior and social engineering, which is why user access remains one of the most frequent attack vectors," he explains.

Risks vs. Resource Allocation

The majority of respondents in the Market Pulse survey understand the challenge at hand. Sixty-five percent say their organization's security strategy starts with internal security measures, not endpoint vulnerabilities. They acknowledge that the biggest potential damage to their business lies at the database layer of their IT infrastructure. Yet among the same group, the allocation of budget is the opposite of where risks are perceived. Two-thirds of IT security resources – including budget and staff time – are allocated to protecting the network layer, with the remaining third split among applications (15%), databases (15%) and middleware (3%).

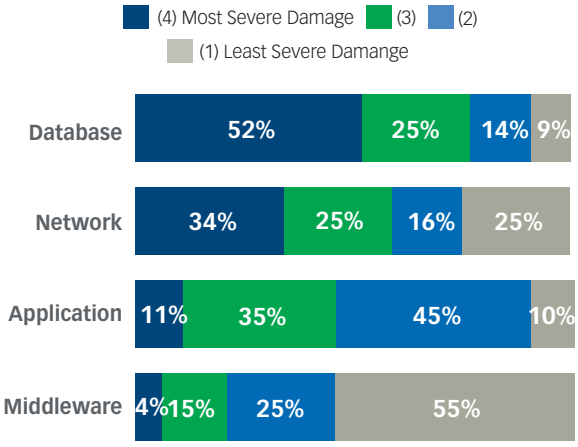
One possible reason: More than 4 in 10 respondents believe database and application data are inherently safe because they lie deep within the perimeter and therefore are more difficult to reach. This is a dangerous assumption. The 2012 Verizon report found that servers were the largest category of compromised assets (64%) and database servers were the source of 94% of compromised records involved in security breaches. Network infrastructure, by comparison, accounted for less than 1% of compromised assets.[2]

"Because we believe that applications and databases are safer, we lower our guard on those systems," says Persaud. "But think about all the people who touch those servers during the course of business. Is the data in your general ledger really secure if multiple database administrators and developers may have excessive access directly to the database layer?"

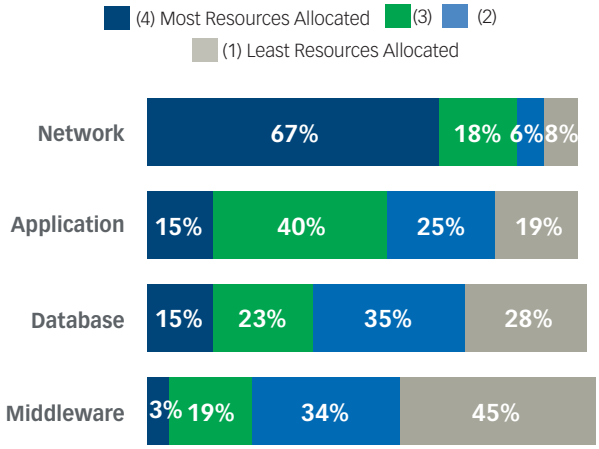
The gap between the threat of severe damage due to a database attack vs. the resources allocated to protecting the database layer is significant – highlighting the disconnect in how organizations are securing their IT infrastructures.

[2] "2012 Data Breach Investigations Report," Verizon, 2012 http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

Threat Represented by Attacks on Vulnerability Layers



Allocation of Resources by Vulnerability Layer



SOURCE: IDG RESEARCH SERVICES, NOVEMBER 2012

Because the network and the perimeter are so porous, security teams that continue to allocate the bulk of their resources to network protection are likely to see diminishing returns on their investment.

"We can't lower our guard on the internal systems," says Persaud. "While criminal threats and cyber attacks are externally driven, they are exploiting weaknesses internally."

Building a Case for Inside-Out Security

One issue for CISOs and CSOs who are looking to revamp their security strategies involves justifying the payback on security investments. In the Market Pulse survey, correlating spending to concrete risk reduction is the No. 1 challenge security managers cite.

An inside-out approach could help security chiefs address this challenge. Protecting data at the source increases confidence that security investments are aligned with the greatest threats. Protecting data in the database would also save both time and money because most of the organization's sensitive data resides in the database. As a result, an inside-out approach would achieve a higher return on their security investment.

What's the best path to developing an inside-out approach to security? Here are three steps CSOs and CISOs can take to realign their resources and increase confidence in the robustness of their security infrastructure.

1. Align business strategy with security strategy. CISOs should develop a clear understanding of the assets that are most strategically important to the business. Most will fall into broad categories: customer information, employee information, corporate financial information and intellectual property. If these assets are compromised, then the entire business is compromised and its value – to customers, partners and, ultimately, shareholders – decreases.

One way to identify these assets – and their level of vulnerability – is to examine every touch point where this information is collected, shared or displayed throughout the organization, along with who inside or outside of the organization has access to the information. This knowledge will help CSOs better understand the risk and educate their C-level peers about the importance of aligning security investments with the greatest risks in language that the business leaders can understand.

"The CSO has to educate the rest of the C-suite about how to protect customer and other business-critical information, as well as the impact of not protecting it," says Persaud. Education also involves positioning security investments as an enabler of business transformation, not simply a deterrent to criminals.

"Security removes the barrier to business opportunity

by securing the participants and their experience," says Persaud. "The CSO must help the CEO, the C-suite and the board incorporate the economics of security into strategic planning initiatives."

2. Revamp processes and privileges. An inside-out approach requires getting a firm handle on user access privileges across applications and databases. While most threats are external, cyber criminals often exploit weaknesses in internal processes, such as lax password policies or single sign-on permissions.

"Hackers know employees are putting weak passwords on systems," says Persaud. "They know multiple people share elevated privileges. They know how to go after system accounts that give them incredible power. Because there are so many vulnerabilities in the controls, once the perimeter is broken, the strategic information is easily accessible."

3. Design for scale. Inconsistency is the enemy of a comprehensive security policy. Decentralized policies make it difficult to react quickly to network attacks and propagate patches or security enhancements across the enterprise. Criminals will find the weakest points quickly – often faster than IT can react. The challenge is particularly acute in emerging markets where perimeter security may not be as advanced as in more mature markets.

INSIDE-OUT SECURITY BUILDS TRUST, AND TRUST DRIVES THE BUSINESS. AS MORE BUSINESS IS CONDUCTED THROUGH THE CLOUD, VIA THE WEB AND MOBILE DEVICES, TRUST BECOMES EVEN MORE OF A COMPETITIVE DIFFERENTIATOR. THE BRAND THAT IS THE MOST TRUSTED WILL WIN.

"Consistency in security is enabled by scalability, and scalability can only be achieved by automated administration and governance," says Persaud. "You need access controls in Asia to go into effect as soon as you launch them in North America. If the security is compromised from an attack in any region, we have to propagate the fixes consistently in all geographies simultaneously. Otherwise, the attackers will replicate the attacks in other geographies faster than we can respond."

The rise of mobile devices in the workplace makes the need for scale even greater. Mobile identity management policies that minimize or eliminate locally stored passwords – especially those stored in plain text – should be part of any mobile application deployment strategy.

Summary

A recent article in The Wall Street Journal explains how a "trust deficit" among businesses, policymakers and consumers – stemming from the global financial crisis – continues to inhibit economic growth.[3] The same is true regarding cyber security. IT security will determine the level of trust consumers and shareholders have for new business initiatives. Whether you are launching a new online brokerage in China or an online grocery delivery service in the United States, securing the participants and their experience will determine the level of economic activity, the value of the brand and the quality of the firm's reputation. A comprehensive approach to security can play a role in helping businesses regain some of their lost trust with customers – beginning with customer data security.

"Many of our interactions throughout the day – from withdrawing cash at an ATM to checking my email to opening an app on my iPhone – involve an element of IT trust," says Persaud. "When that trust is broken, consumers do fewer transactions."

Inside-out security builds trust, and trust drives the business. As more business is conducted through the cloud, via the Web and mobile devices, trust becomes even more of a competitive differentiator. The brand that is the most trusted will win. CSOs and CISOs play a key role in building brand trust by delivering and maintaining secure environments for conducting business.

It's safe to assume that the risk at the periphery can never be truly eliminated. So it's up to security teams to reprioritize around their business's most critical assets: its data and applications. By developing an inside-out approach to enterprise security, CSOs and CISOs can turn security into a key enabler of business transformation. ■

[3] "How a Trust Deficit Is Hurting the Economy," The Wall Street Journal, Jan. 27, 2013