acmqueue The Theft of Business Innovation: Overview

An overview of key points discussed in the joint ACM-BCS Roundtable on Threats to Global to Competitiveness.

The joint ACM-BCS Roundtable on Threats to Global Competitiveness focuses on the new business security realities resulting from having practically all business information directly or indirectly connected to the Internet and the increased speed and volume of information movement. This new environment has enabled an entirely new dimension in what has been considered important business value-creation assets and in the criminal ways that information can be stolen or used to harm its owner. What follows are the key points from that broader conversation. For a more in-depth look at what the roundtable covers, read the full panel discussion. —*Mache Creeger*

THE NEW THREAT LANDSCAPE

The speed and volume of data that can now be stolen from a business has enabled criminals to take a comprehensive snapshot of all that business' operational data and implement it at another location. While past high-value commercial information has been more along the lines of banking codes or secret inventions, today's criminals have broadened that definition to include the more mundane but valuable information such as manufacturing processes, suppliers, customers, factory layout, contract terms, employment data, and general know-how.

As a result, given that almost all business information is either directly or indirectly accessible by the Internet, any business—regardless of size—showing leadership in any aspect of its industry can now become a lucrative target for attack. With this information in hand, attackers can sell state-of-the-art competitive advantage to anyone who can set up equivalent businesses without the original upfront time and/or money investment. Here are some examples:

- A relatively small regional U.S. furniture company—not a business you normally think of as having key intellectual properties—became an international target. This company had its furniture designs stolen by a Southeast Asian furniture manufacturer that went on to undercut the prices of the U.S. company.
- Attackers broke into U.S. chemical plants and refineries and copied every bit of operational plant data they could: how everything is connected, all the control systems, and settings for every pressure, temperature, switch, and valve. Soon after, new facilities in those very industries popped up in Southeast Asia. No visitors are allowed because, it is believed, they are exact replicas of the facilities that were attacked.

How far ahead of its competitors a business is directly correlates to how much money the business makes from its market. For a typical manufacturing facility, it is reasonable to assume a 5 to 15 percent cost reduction each year for the first six years of operation. Those savings usually represent a majority of the profits. Using stolen operational information to create a competing duplicate facility essentially steals those profits from the original business.

Frequently localized to specific geographies, criminal communities often specialize in stealing information from particular companies or, sometimes, entire industries. Benefiting from this type

of information, however, requires people who understand Western business practices—a Western education and experience working in Western industry. This limits the utility of stolen information since that type of experience is not readily available in the countries where these activities are most prevalent.

PAST WISDOM NO LONGER VALID

Security was once the province of national intelligence agencies focusing on defense/national security-related information theft. Today next-generation private organizations have spun off these security services for hire. Traditionally the business community has viewed information security as at best a supporting service and at worst a grudge purchase, rarely aligning security with the processes that create business value. While companies are sensitized to the confidentiality of their traditional intellectual property, they are usually not sensitive to the confidentiality of their control systems, corporate e-mails, sales and marketing, human resources data, or other types of information.

Past security wisdom mirrored the old saying: *When chased by a bear, you don't have to outrun him, just the person next to you.* Implementing enough security to encourage attackers to go elsewhere is no longer a valid strategy. Being targeted today means that attackers who are after something specific will probably not go away until they get it. In this high-paced threat environment, do not assume that if your business is ranked number 963 you are too far down the list to be attacked. You will be attacked, and probably sooner rather than later.

ADVICE

What makes an organization an attractive target is market-sector leadership in a particular industry—for example, technology, cost, style and fashion, or even aggressive new market expansion. Along with providing basic security such as firewalls, antivirus, intrusion detection, etc., you should view your organization as an attacker would and determine which information assets provide attractive value-creation benefits to potential competitors. Theorize an attacker's motivations, and in making this analysis, do not rule out destruction of reputation and/or data integrity as another way an attacker could benefit from a breach.

Build a security vulnerability matrix that defines the five steps an attacker must take to be successful:

1. Find the target.
2. Penetrate it.
3. Co-opt it.
4. Conceal what you have done long enough for it to have an effect.
5. Do something that can't be reversed.

List all the components of your information system such as hardware, system software, networks, and critical applications; and, given the above steps, itemize your business vulnerability (why might you be a target?) plus the corresponding attack tools and their countermeasures. Do not limit this review to senior management; involve a broad cross section of your organization, including lower-level employees—they usually have the best insight into what is critical and what is vulnerable. Developed by our panelist Scott Borg, this approach will help in addressing security in a more comprehensive manner. Often people find that they put most of their effort into penetration prevention and backup, leaving many other areas undefended.

Far too many organizations spend their security resources protecting the network perimeter (firewalls and other fairly low-level things such as the protocol stack). The majority of today's threats are happening in the application layer, but many applications do not have logs, making the monitoring of this area of vulnerability all the more difficult.

When breaches occur, you need to be in a position to understand what happened as quickly as possible. Information systems should be architected on the assumption that breaches will occur, and functions needed for proper response should be an integral part of the design. Security infrastructure should focus beyond technical detection and include related metadata so that events can be interpreted in a context that makes sense to the business. Ask questions such as: If a person logged into a network, what physical location was reported? Did it correlate with the physical access-control log reports?

Many security-detection tools, while providing comprehensive information, show that information in a narrow, non-contextualized way. Similar problems may result when security is overseen only by the IT department, rather than also having a more business-centric focus from the operations director or the board.

Hiring a penetration testing organization will give you an independent assessment of your organization's vulnerabilities. Be advised, however, that these groups always find something, and it is important that people understand the context of what is found, distinguish what is important in addressing the issues raised, and get to a known baseline within your industry.

Outsourcing information services to cloud-computing vendors could be a good thing for small companies and maybe even midsize companies, as it is probably the first time those companies are instituting some level of professional management and 24/7 monitoring. Customers need good methodologies to compare the security models offered by the various vendors, however, and that is extremely difficult to find at this stage of the cloud-service provider marketplace.

Make sure that your employees are motivated to protect the most important value-creation aspects of your business. Do not give them incentive to choose limited short-term benefit over longer-term catastrophic loss.

Don't be afraid to talk to other folks in your industry. Partners/competitors are being exposed to the same types of threats, and all have a vested interest in lowering the industrywide threat level.

Security professionals should be an integral part of the senior management of an organization. Given that practically all of its information assets are directly or indirectly connected to the Internet, the ability of a business to secure its value-creation aspects is critical to its survival and growth.

Security threats have evolved to include a broad spectrum of organization sizes and industries. No longer limited to large companies with highly specific information assets, any organization that shows leadership in its field needs to guard its value-creation information aggressively by taking concrete steps toward its protection.

Because every organization is either directly or indirectly connected to the Internet, no one is really beyond the reach of attackers. Taking the advice offered here will place you in a better position to disrupt an attack when it occurs. ◻

LOVE IT, HATE IT? LET US KNOW

feedback@queue.acm.org

© 2010 ACM 1542-7730/10/1100 \$10.00