Clear and Present Danger: Cyberattacks, Hackers and the Increasing Threat to Information Security

Earlier this year, Google disclosed that its network infrastructure had been compromised by a sophisticated cyberattack that resulted in the loss of sensitive intellectual property. Unfortunately, the incident was just the tip of an iceberg. Soon after Google's disclosure, U.S. investigators studying the incident told The Wall Street Journal that the prime suspects behind the attack may have been involved in attacks on more than 30 other companies. As Richard Clarke, former U.S. counterterrorism chief, put it at the RSA information security conference held earlier this year in San Francisco: "Every day we are being attacked. Every major company, [and] every major institution, [have] been penetrated."

Who is behind the attacks? Experts say the reality is that there are so many different potential suspects to worry about -- ranging from nebulous groups of hackers, to organized crime, to competing corporations, to nation-states and military agencies -- and frequently even the motives for the security breaches are unclear. This leaves victims and investigators alike wondering both who was behind an act and why. Investigators, however, are certain of one thing: that cyber attacks and the vulnerabilities facing business and society today are intensifying, and even approaching pandemic levels.

Unfortunately, according to experts in the industry, providing a sufficient level of protection is becoming more and more challenging. "Security is always a cat-and-mouse game between hackers and security vendors," says Kartik Hosanagar, a professor of operations and information management at Wharton. "What has changed is that both companies and hackers have grown sophisticated. So the good news is that most security software will protect us from the most basic threats, which was not the case in the past. But the bad news is that malware and viruses have become more sophisticated, so even advanced users can fall prey to them." Worms associated with interactive media and malware affecting social networking sites are particularly dangerous, he notes, because "for example, you are less likely to be suspicious of a message from a friend on Facebook asking you to click on a video link. And yet, this kind of attack is on the rise" even as Facebook, Twitter, and other such sites are increasingly being used by businesses.

So-called botnets give some indication of the scale of the problem. Botnets are networks of computers unknowingly infected with software enabling them to be controlled by a third party (known as a "bot master") for massive, coordinated attacks. Analysts estimate that there are now millions of botnet-infected computers around the world, running in homes as well as businesses. In one example, Spanish authorities in May said they had come across a far-reaching network of compromised computers tapping into credit card and banking data from more than 12 million
PCs -- including, reports said, PCs inside more than half of the Fortune 1000 and in more than 40 major banks.

Similarly, in the Google case, the suspects that investigators focused on have a history of primarily attacking corporations -- as opposed to the U.S. military or other government agencies, an unnamed source told *The Wall Street Journal.* These hackers steal specific data and intellectual property, the source said, rather than simply taking anything and everything they can access. For many executives, this was a chilling revelation, indicating that the threats to their business may be far more sophisticated and strategic than assumed. As George Kurtz, McAfee's chief technology officer, told *The New York Times*, "Data has value ... If companies had this [lack] of security in their cash-management systems, they'd be broke." As if underscoring the point, in June a group of hackers disclosed that it had obtained the e-mail addresses of more than 100,000 owners of 3G Apple iPads, by exploiting a flaw on AT&T's website.

**New Threats, New Challenges**

Experts say that the recent attacks on information security suggest at least three things: First, that hackers increasingly know exactly what they want, while their targets often struggle to understand the threat or where it is coming from. Second, that attackers continue to rapidly develop new ways to access what they want, and as a result, the threats can come from anywhere. (For example, *The New York Times* disclosed this year that hackers were trying to use online advertising on the newspaper's own website to disseminate malware.) Finally, observers believe that almost everyone and every company ultimately is at risk, a result of today's highly networked global economy and communications infrastructure.

Meanwhile, the attacks themselves also are getting both more sophisticated and more targeted to going after critical information. As a result, Hosanagar and other experts say the so-called malware used by hackers and the like is being designed to avoid detection, to survive longer on targeted machines, to recreate itself if parts get destroyed and to send back a bigger payload of data. The "bad guys" are building malware rapidly, observers note, using the same sophisticated programming tools available to the "good guys" trying to stop the attacks from happening. In addition, there are a lot of different potential attackers coming from different places -- they all have unique motives, yet their attacks often look the same, so victims are unable to tell from the incident either who the perpetrator was or what the motive was, which makes it hard to figure out how to respond. All of this means that many experts believe that traditional ways of securing a company's information assets are no longer sufficient.

At the same time, behavioral shifts come into play. As boundaries between organizations, and between work and private activity, continue to morph, the ways in which users need to access information is changing, which means there are now many more potential points of weakness. Indeed, experts say, many organizations do not know all of the applications that are running on their networks at a given time -- and thus, where they are vulnerable. Businesses are also in a constant state of change due to acquisitions, spin offs, divestitures and even employee turnover. In addition, with the increased use of remote employees, contractors and visitors, IT professionals not only have to keep track of employees using company-issued devices, but also non-employees and non-company-issued devices. The amount of data within and flowing
between companies is increasing exponentially, which means IT security measures need to protect more and more kinds of information, on an increasing number of devices.

All of this contributes to the growing vulnerability of even the most resource-rich companies, experts say. Google, banking giants and retailers (who have lots of credit-card information on file) may be some of the most dramatic targets, but at the same time every company, in every industry, holds a vast amount of highly valuable data, whether it is account information, product design information or anything else. Symantec's latest State of Enterprise Security report, released in February, reported that 75% of organizations surveyed suffered a cyberattack in the past year. As a result, 42% of enterprises ranked Internet-related risks as their biggest risk concern -- more than natural disasters, terrorism, traditional crime and brand-related events.

**Fighting Back**

From a corporate perspective, experts say the required response to these threats has two sides. The first is protecting IT infrastructure, meaning the systems, hardware, software and networks used by an organization. The second involves protecting the actual information or data that is supported by that infrastructure, whether the information is in motion, in use or in storage. Complicating those efforts, however, is the need to protect the business environment while ensuring that employees have access to the information and services they need to do their jobs.

As with any other costly undertaking, companies want to ensure that they don't break the bank, especially in the current economic climate. What it all adds up to, observers note, is IT departments that must handle a growing number of information security threats, all increasingly sophisticated, with very little or even no additional budget or resources. But that may be changing. "There is a clear move toward -- and a much more significant interest in -- better understanding the risks associated with IT by directors and senior management teams," states Erwann Michel-Kerjan, managing director of the Risk Management and Decision Processes Center at Wharton. One reason for that, he says, is an overall increased focus on risks and risk management as a result of the large number of catastrophes and crises companies have seen unfold in recent years, from natural disasters to financial meltdowns. "We have witnessed companies going under, or being severely hit, due to a single untoward event. As a result, how to better manage and finance extreme events is now a question discussed by many more board of directors than five or 10 years ago."

In addition, Michel-Kerjan says, many organizations have recently created C-level positions, such as a chief security officer responsible for IT protection issues, because technology and the threat landscape are changing so rapidly that specialists are needed to guide companies' responses. However, research suggests there is still a lot of work to do. For instance, a recent survey of 80 chief security officers and over 200 members of ASIS International (a leading trade association for corporate security professionals) found that 40% of the responding companies had no executive with primary responsibility for coordinating risk-management strategy. "That's hard to believe," Michel-Kerjan points out, "given that extreme events and risk management are making headlines almost every other day."

**Advances in Digital Security**
Companies developing solutions to the information security problem can basically be divided into two camps. In one camp, there are the focused, specialist players, either leveraging an expertise in one or two specific areas, such as e-mail security or data-loss protection, or working across a broad range of key security issues. Some of the biggest companies in the latter field are Symantec, McAfee, and RSA -- the security division of information infrastructure company EMC -- with a great deal of startups rounding out the scene. "Security cannot be bolted on as an afterthought." says Brian Fitzgerald, vice president of marketing at RSA. "It must be embedded directly into solutions and infrastructures by design."

In the other camp, almost all of the tech industry heavyweights are making security a core part of their strategy. Cisco, Google and Microsoft have all made targeted acquisitions of e-mail security vendors over the last few years to beef up their internal development, and today all these companies are now among the leaders in the market segment. Other big players such as Oracle (which recently bought Sun Microsystems) and IBM also are going after security business, especially from an identity management and access space.

One increasingly critical focus area is in "the cloud" as more and more companies essentially outsource some of their IT infrastructure to Internet-based utility computing models, where software applications and services are provided on demand. Here, monitoring and controlling access to information become even more challenging, as systems must be able to work both in-house and virtually, especially in cases of multi-tenant systems, where several companies or accounts may have sensitive information managed by a single server. CIO magazine recently reported that 51% of CIOs cited security as the greatest concern surrounding cloud computing.

Cloud providers are already responding to those fears. "In the past, cloud providers hesitated to provide security guarantees and rarely negotiated contract terms related to security guarantees. However, more and more they compete based on their security commitments" Wharton's Hosanagar notes. "Companies that adopt cloud services are increasingly asking for strong encryption without compromising speed or performance, and clearly-specified [compensation for] damages in case of a breach."

Microsoft provides another glimpse of what's next. The software giant initially focused on solutions to protect PCs, but over time has expanded its focus to include the broader tech ecosystem and threats to computers in home and corporate settings, Earlier this year, Microsoft attorneys won a court order to take offline more than 200 Internet domains that were at the center of a large botnet, dubbed Waledac. Microsoft estimated that the botnet had been sending up to 1.5 billion spam messages a day, and was a major source of malware on the Internet.

Still, Microsoft acknowledged that the Waledac takedown was only a partial solution. "It's not a remedy because it's reactive," Scott Charney, vice president of Microsoft's Trustworthy Computing group, stated at the RSA conference. "The next question is, what can we do proactively?" It was a sentiment echoed by Janet Napolitano, secretary of the U.S. Department of Homeland Security, at the same conference. "We can't be static because we don't live in a static world."

Designing an Integrated Approach
Looking ahead, experts say more and more companies will approach information security risks in the same way they deal with other major threats, and in a much more integrated fashion. "Risks are becoming more interdependent, and we are more and more dependent on our IT systems -- supply chain and telecommunication systems in business are more interconnected today than ever," notes Wharton's Michel-Kerjan. "But we cannot protect everything, everywhere, all the time. Ask yourself: How much could it cost if things go really really bad? Risk financing and board preparedness are two keys elements of success and economic sustainability."

To better prepare top decision makers and boards for cyberattacks or other security breakdowns, Michel-Kerjan suggests that companies take a page out of the playbook for how corporations manage effectively in response to natural disasters, terrorism or even pandemics. One approach often used in military scenario-planning exercises, for example, is to split key participants into two teams and run a one-day exercise where one team cooks up potential cyberattacks while the other team designs a response. "You will be surprised by how imaginative your employees can be about what is your true weak link," Michel-Kerjan points out. "Keep in mind here that what can seriously hurt you will not be a 'usual' scenario."

Finally, because effectively combatting cybersecurity challenges are just as much about office culture and people as technology, Michel-Kerjan argues that, as with any major risk, it is essential that the CEO attends and plays his or her role during the whole scenario-planning exercise. "Too often the CEO is 'too busy' to do it, and ends up never being trained for dealing with extraordinary situations. In addition, think about what signal the absence of the CEO sends to the employees about that issue. Most likely, she or he does not think preparing for it is really important. So, if that's the case, why should they?"

This is a single/personal use copy of Knowledge@Wharton. For multiple copies, custom reprints, e-prints, posters or plaques, please contact PARS International: reprints@parsintl.com P. (212) 221-9595 x407.