strategy+business

ISSUE 83 SUMMER 2016

Safety in the Cloud

The next generation of cybersecurity prevents attacks by monitoring online behavior — of intruders, customers, and everyone else.

BY DAVID BURG AND TOM ARCHER

REPRINT 16208

pwc | strategy&

Safety in the Cloud

The next generation of cybersecurity prevents attacks by monitoring online behavior — of intruders, customers, and everyone else.

by David Burg and Tom Archer

For most businesspeople, the word *cybersecurity* suggests a shield. When people think about protecting their enterprise from intrusion with information technology, they typically think of the much-publicized breaches of the past few years: those at Target, Sony, JPMorgan Chase, Goodwill Industries, Snapchat, the U.S. Office of Personnel Management, and a wide range of other organizations. It's understandable that most companies take a defensive posture with respect to digital security. They know that hackers from around the world are continuously probing corporate networks, looking to steal data of value — information about customers, personnel, finances, proprietary research, trade secrets, and other critical assets — and to compromise their technology in other malicious ways.

But imagine a different kind of cybersecurity, one that no longer depends strictly on the IT department's engagement in a desperate, never-ending arms race with intruders. Instead, a company would use cybersecurity as a way to better understand its business environment. It would defend itself by monitoring activity across all its online systems, studying not just the moves of hackers but the actions of legitimate customers as well. Both types of visits, after all, are forms of repetitive human behavior, opposite sides of the same coin.

This approach would use technology to sense and respond to threats, and it would be just as effective — indeed, more effective — at eliminating vulnerabilities. But it would not be a purely technological or defensive solution. Nor would it view digital intrusion as a siege that must be defended against, at considerable cost. Rather, it would embrace an entirely new concept of cybersecurity as a source of strength — that is, as an opportunity to rethink the foundations of a company's operations and customer relationships. If your company followed this approach, you would monitor attacks through sophisticated pattern recognition, deflect them through the use of digital decoys, and learn from any attacks that did occur, in order to better prevent future threats. You would also gain a richer understanding of your business environment, and a better sense of what legitimate customers want and need.

Cybersecurity of this type exists today. The key is cloud computing. For many companies, keeping data in the cloud has become a fact of life. But some business leaders — even as they recognize the benefits of greater operational agility, lower cost, and adaptability that come with the cloud — continue to express concerns about its security. They worry that they will have less control over sensitive corporate data when it is stored in remote inter-

Moving to the right kind of advanced cloud system represents a more dynamic approach to risk.

Illustration by Lars Leetaru

linked computers. They assume that computer firewalls are like locks on a brick-and-mortar door: The more solid the barrier, the more impervious the system.

The truth is that applications and data maintained in the cloud can be *more* secure than data held in on-premises corporate systems. That's because moving to the right kind of advanced cloud system represents a more dynamic approach to risk. The security of your enterprise is based not just on keeping people out, but on watching people who come in. You learn from every attempted attack and even from every use of your data. You integrate cybersecurity with marketing, customer service, and logistics, to develop a single way of tracking the behavior of everyone who interacts with your company. With this type of system, the more attacks the cloud faces, the stronger it becomes.

The Best Defense Is Analytics

The standard approach to protecting on-site corporate networks from cyber-attacks involves the use of IT systems to detect and prevent unwanted efforts to gain entry. Such efforts are premised on the conventional view that a company's network is like a castle inside walls. The castle is protected by bolting on more and more security measures in hopes of keeping out the bad guys without rendering these networks so impervious as to make them unusable.

Yet no such purely defensive tactical system can ever be truly effective, especially as companies digitize more and more aspects of their internal operations and external contacts with the outside world. Operational technologies are becoming too complex to be protected this way, and hackers will always be one step ahead. The problem calls for an entirely different type of solution, and that's where the cloud comes in.

It's important to note, before going any further, that not all cloud-based systems are equal. Some are more advanced than others. Some services billed as "cloud computing" do little more than replicate an on-premises installation in a network of interlinked computers. When we talk about *the cloud* in this article, we are referring to offerings such as Google Cloud Platform, Amazon Web Services, and Microsoft's Azure. These advanced cloud services represent major investments in interoperability, protections, and ongoing innovation that allow off-premises enterprise IT to realize its potential.

No purely defensive system can be truly effective. Technologies are too complex, and hackers will always be one step ahead.

From a pure security perspective, the virtues of the advanced cloud are many. It can provide almost unlimited low-cost computational power, which is often needed to identify the kinds of suspicious activity that indicate the movements of hackers and who they might be. Without the cloud platform and its analytical power, it would be almost impossible to detect such patterns, especially when monitoring huge volumes of data, highly complex and interconnected applications, and time intervals as long as months or years.

Because cloud software is independent of particular hardware platforms, it is innately "virtual" — code runs on other code, not on devices. This makes it easier to adapt, often immediately, to intrusions and other changes in the environment.

The cloud also offers simplicity. It creates fewer points of vulnerability and makes it easier to keep up with technological advancements — because companies can now rely on their service providers to build the infrastructure, hardware, software, and services required. It also enables companies to scale up their systems as needed, to a degree not possible with on-premises computing.

For example, Bluecore, a New York City–based startup, provides about 100 high-end e-commerce companies with the ability to send customers emails in response to their online behavior. A shopper might make several purchases on a website, but then reach the shopping cart page, feel put off by the shipping costs, and fail to complete the transaction. Bluecore's app can detect that motive in the online behavior of the customer; it can also be set up to send an automated, personalized response that, say, offers to waive shipping costs. According to Bluecore cofounder and CTO Mahmoud Arram, the ability to track security was a critical factor in the company's use of cloud computing — in this case, of Google Cloud Platform. "One of our customers

needed confirmation of certain levels of security, and we were able to show them that we could meet their security requirements," he says, in a report that Google produced. "It made me realize that if we were running our own data center, we probably would have run into trouble in that regard."

Most importantly, a cloud-based system offers vast improvements in a company's ability to counter cyber-threats because of the way it responds to intrusion. A typical cyber-attack begins with a hacker detecting a vulnerability in a company's systems or network that allows the intruder to plant malware on a computing device. The malware may never have been seen before. It is very hard to detect; the so-called command-and-control computer that manages it and receives information from it could be located anywhere in the world. The malware is designed to move through the company's IT systems, profiling their data structures and the information they store, and then to copy or remove any valuable data it finds, transferring it to the command-and-control hardware.

By the time a cyber-attack is detected in a typical computer system on your premises, the security technologies have already failed in at least three ways. The perimeter technology failed to keep the unauthorized activity out; the network technology failed to detect the ongoing communications between the command-and-control computer and the infected end points; and the end-point technology failed to detect the malware as well as the suspicious behavior occurring among the end point, network, and perimeter.

The standard defense against such attacks is limited to remediation and repair. First, the malware is removed anywhere it can be found. Then the vulnerable points must be repaired and the losses and damage assessed. Since many on-premises IT technologies are not designed to work with one another, any analytical capability that the company's systems have can't pull together the pieces of the puzzle to "see" and "understand" what is happening, so it's highly difficult to learn from this experience. Instead, there is always another cybersecurity application the company can bolt on, as it hopes for the best next time.

In the cloud, by contrast, security technologies are fused together into an analytics platform, which is maintained across a wide variety of computer hardware systems. In real time, the system logs and analyzes all activities taking place on the computers, including all clicks, keystrokes, and Web requests. An advanced cloud service can then compare this activity against its own continuously compiled repository of intelligence about large threats — as well as an ever-expanding group of algorithms to detect anomalies. The system also continually checks the integrity of the security controls in place, and evaluates the critical entry points of the system and what alternatives might exist if they had to be shut down.

The moment a new threat is identified, the operational data about the hazard is injected into the analytics platform and compared to the entire body of accumulated security technology information. At the same time, any threatened applications and their associated data are immediately respawned in a new, software-defined network beyond the reach of the attackers, and the vulnerability is immediately patched.

The result is a dramatic reduction in the time elapsed between detecting and countering the threat. Moreover, because all interactions with cloud-based applications are browser-based, users must be authenticated each time they log on. This authentication information, and the increased information about the browser session itself, adds to the analytics firepower of cloud-based security. Any damage assessment necessary is minimal, and remediation is almost instantaneous.

Frontiers of Cybersecurity

When companies move their cybersecurity to the cloud, they typically start by leaving some applications — typically the most valuable, whose breach would create the most problems — on their premises. But your company can't fully reap the benefits of this new approach until it makes a cloud-based cybersecurity program an integrated element of its overall analytics program and business operations. You may have moved other aspects of your digital activities into the cloud already. Now is the time to integrate cybersecurity fully into the mix.

The best way to begin is by analyzing how your organization operates, both internally and externally. Identify how the key people you need to protect, including the customers and employees whose sensitive information you handle, work and communicate. Where are they usually located? Where are they traveling to? You'll want to secure those locations. Who's coming to work, and in which offices? Look at the devices they use to connect with you, the systems in your own back office, and the communication patterns of everyone involved.

One primary goal of this analysis is to set up early indicators of intrusion. Hackers can often be recognized through their entry credentials, machine identification, geolocation, and (increasingly) biometric data — as well as how they behave online, where they go, and what they appear to be looking for. Moreover, every individual has an "electronic fingerprint" based on the pace, rhythm, and recurring sequences of their keystrokes. Analysis of all these patterns can help companies detect criminal intruders and the bots that make up more than 60 percent of the traffic on the Internet — before they do any damage.

Another primary goal is to identify and understand the people you should be engaging with (customers, suppliers, partners) and distinguish them from the people out to do you harm. For example, you might analyze your presence in supply chain networks and the vulnerabilities to which they expose you. How can you optimize, protect, and monitor those logistics? What kinds of efficiencies will arise as you look for ways to streamline your contacts with outsiders?

You can also integrate cybersecurity with insights into customer behavior and preferences. The task of monitoring intruders' efforts to break into your online systems is very similar to the task of authenticating legitimate entrants as they log in and move around your websites. A single cloud-based analytics system can monitor the activity of customers, employees, and intruders simultaneously. The resulting insights can enable your company to paint a picture of all the activities going on in your systems, good and bad. This picture will become ever more detailed as the system gathers more data by tracking online behavioral paths, detecting threatening patterns and anomalies that humans simply can't see. It can then devise further heuristics to counter those activities. A great deal of cybercrime involves low-probability events that have a high impact — just the kinds of activity that big data analytics is especially good at pinpointing.

The final strength of the cloud-based system lies in its ability to combine authentication and analytics from multiple sources. As the problem of cyber-attacks becomes increasingly shared among companies and governments, it will be important to openly exchange information about the attackers' identities and the nature of the threats they pose. With a cloud-based system, this can be done without compromising anyone's secure data, and it can be set up in a way that benefits the entire knowledge base shared by cloud participants.

One industry that relies on integration is healthcare, wherein concerns about cybersecurity and legal protection go hand in hand. The organizations that make the integration work are those that build a single system, sometimes from multiple cloud vendors, that incorporates patient information, operations, and regulatory compliance. For example, Beth Israel Deaconess Medical Center in Boston, a teaching hospital of Harvard Medical School, has publicly explained the transition it is making, which it is undertaking in part because the lease on the building housing its data center is about to expire. Instead of seeking a new facility, Beth Israel "embraced the public cloud," as chief information officer John Halamka put it.

Halamka, who is himself a practicing emergency physician, arranged for an independent audit of security issues at three vendors — Amazon, Google, and Athenahealth, an electronic services company that specializes in this industry and that is also moving rapidly toward the cloud. Halamka checked into the physical security of the vendors' data centers and their encryption, as he would with any stand-alone system. But the compelling factors had more to do with the ability of the system to maintain regulatory standards for patient confidentiality, to improve administrative tasks, and to track behavior. "Encrypting data is sometimes seen as a panacea," he wrote in a blog post about the subject, "but if we study the major security breaches of the past year, we'll find that most accesses occurred at the application level, not the data level — encryption of data [in itself] would not have helped."

Netflix decided that converting most of its operations to the cloud would free up its engineers to focus on creating new services.

Making the Move

Moving a corporation's technology infrastructure into the cloud is an enormously attractive proposition,

and the promise of cloud-based cybersecurity only makes it more so. It can allow your company to avoid spending the millions of dollars that would be needed to bolt more security onto your on-premises systems. The capital saved this way can be put to better use funding the move itself.

Among the virtues of moving cybersecurity into the cloud is that it enables you to think of security not as a technical specialty but rather as a truly differentiating business capability. Every company these days must guarantee the security of its customers' data. A company with a distinctive capability in this domain goes further. If it's a business-to-business company, it may offer the highest level of security for clients and suppliers, given the proprietary and often secret nature of the data they exchange. If it's a consumer-oriented company, it may use security, monitoring, and tracking to offer personalized services that no one else can match.

But no large company can make the move all at once, given its investments in massive legacy systems and databases. Instead, it must take a logical, systematic, risk-based approach to protecting its most sensitive data as it moves it to the cloud.

Your first step should be to conduct a pilot program on an application or data set that isn't hugely sensitive or mission-critical, paying attention to what is involved in making the move, how well the system functions in the cloud, and how it is interoperating with the associated cloud-based security systems. Then, once you are comfortable with the pilot, you can begin moving more sensitive data and systems to the new environment.

For each part of your operations, you can build a business case, thinking strategically about the economic benefits of moving your information technology into the cloud and the way such a shift can affect your overall cost management. If you continue to invest in on-premises IT systems, you will trap yourself in the ongoing sunk costs of conventional cybersecurity approaches. Each year, as intruders grow more sophisticated, you'll have to grow more sophisticated along with them. You'll have to invest in countering them. And they only have to break past your defenses once to unleash a horrendously expensive and debilitating attack.

But if you move your IT systems and cybersecurity into the cloud, you'll spend much less on cybersecurity, because you'll be drawing on the expertise of many other companies. You won't have to fund it all yourself. That money can now be moved into more strategically relevant endeavors — which in turn will also help you finance any further cloud-based expansion.

As you plan your move to the cloud, consider the applications and related data that power your most important capabilities, those linked most closely to your strategy. They should be moved first, because they will benefit most from the operational flexibility and analytical power of the new system. This capabilities set might include customer service, consumer insight, logistics, or innovation. Financial systems and data that are sensitive, but that do not support distinctive capabilities, can be moved later.

This is the approach Netflix took in moving most of its systems to Amazon Web Services, just as the company's business model shifted from mainly mailing DVDs to mainly streaming video. The switch began back in 2010, when Netflix decided that converting most of its operations to the cloud, including the actual streaming of content — which at peak times accounts for 37 percent of all Internet traffic — would free up its software engineers to focus on creating new services rather than managing its systems. In the summer of 2015, the company finally shuttered the last of its own data centers, although it still maintains several in-house commodity systems, such as human resources.

Netflix's data is sensitive because in addition to billing information, it contains lists of subscribers' movie preferences and a history of what they have watched. The move to the cloud represented a recognition that this was the only way to protect the company's 62 million subscriber accounts in the face of a rapidly changing and growing operational environment. Netflix is a firm believer in applying the concept of development operations — a combination of agile software development and automated software releases — to constantly maintain and improve its cloud-based security. It has developed several security

The cloud enables you to think of security as a truly differentiating business capability.

applications of its own. These include Security Monkey, which constantly monitors and analyzes the company's security efforts; and FIDO, or Fully Integrated Defense Operation, which automatically analyzes and prioritizes security events depending on their severity. Although no system is foolproof (indeed, Netflix has experienced the leakage of customer passwords onto public websites), the cloud has enabled the company to respond quickly to such events, while maintaining its ability to design and implement new services quickly and efficiently.

Netflix is just one of a number of enterprises with significant cybersecurity concerns that have moved their operations this way. Another example is Apple, which runs its iCloud services on multiple systems including Amazon's S3 and Microsoft's Azure — storing not just credit card data but information on video, music, and book purchases. This approach is noteworthy because Apple tends to be very deliberate in its choices about both outsourcing and security.

Google's cloud platform, for its part, lists a variety of enterprises that base their operations in the Google cloud. They include Autism Speaks, which maintains a massive database of DNA samples linking family genetics to the possibility of learning disabilities; Image32, which allows doctors to share visual images of X-rays and CT scans, always under strict patient privacy rules; the American Precious Metals Exchange, which serves millions of customers in buying and selling such commodities as silver, gold, platinum, and palladium; Brand Vegas, which sells 2,000 tickets per minute to attractions in Las Vegas, including to some of its risqué nightclubs; Energyworx, which compresses and stores electric power usage data from European homes and businesses; the Khan Academy, which provides video courses to students around the world, and keeps track of their onscreen behavior; and Workiva, an online service used by companies to compile and analyze the highly sensitive data that goes into their annual reports. If any of these enterprises got caught in a cyber-attack and had its private information leaked to the public, much of its business would likely be destroyed.

Within the next five or six years, we expect that most companies will fully integrate cybersecurity into their digital business processes. If your company is one of the first, it will help you outpace your competitors. The combination of advanced technologies and cloud architectures will enable your business to respond more flexibly to the changing business environment, to understand your customers in greater depth, and to innovate at faster velocities, all at lower cost — and all while keeping your data more secure. +

Reprint No. 16208

David Burg
david.b.burg@us.pwc.com
is a principal with PwC US. Based in McLean, Va., he leads PwC's global and U.S. cybersecurity practice. He helps corporate clients, law firms, and the U.S. government in matters involving cybercrime investigations, complex data analysis, and operational initiatives.

Tom Archer
thomas.archer@us.pwc.com
is a partner with PwC US and serves on the board of partners for the global PwC network. Based in Silicon Valley, he is PwC's leader for its global alliance with Google. He was previously the U.S. leader of the PwC technology industry practice, and has advised multinational technology companies for more than 25 years.

strategy+business magazine
is published by certain member firms
of the PwC network.
To subscribe, visit strategy-business.com
or call 1-855-869-4862.

- strategy-business.com
- facebook.com/strategybusiness
- linkedin.com/company/strategy-business
- twitter.com/stratandbiz

pwc | strategy&