PROLIFICS WHITE PAPER

Prolifics

PREVENT AND DETECT CYBER-ATTACKS FROM THE INSIDE OUT WITH A REAL-TIME LOOK AT WHO ACCESSES YOUR NETWORK

Author:
Natalie Miller

September 24, 2014

AT-A-GLANCE

MULTILAYER

Security across governance, identity and access management and monitoring

INSIGHT

Systematically track and understand events with log context and complex rules

SECURITY

Protect against external and internal threats with the new perimeter of security

Executive Summary

Data thefts and security breaches can cost organizations millions of dollars, both directly and indirectly, from the loss of data, customers, and jobs to lawsuits and damaged reputations. Organizations are more at risk than ever in a business climate where government regulations are tightening and security threats are more sophisticated.

Yet executives are unable to procure budgets for security infrastructure implementation, and often don't fully understand the complexity that is involved in getting the job done. This whitepaper examines the strategies behind a multi-tiered defense and how Prolifics' Identity Intelligence Solution leverages security rules to minimize the detection time of security breaches.

About Prolifics

Prolifics, an IBM Premier Business Partner and multi-award winner for technical excellence, creates competitive advantage by delivering customized, end-to-end Business Process Management, Integration, Mobile, Big Data and Cloud solutions that achieve business success.

For over 35 years, our technology expertise, industry-specific insight and certified technology accelerators have transformed organizations around the world by solving complex IT challenges. Our expert services include architectural advisement, design, development, and deployment of tailored solutions that empower businesses around the world to create flexible business services and build agility into their organizations.

Premier Business Partner IBM

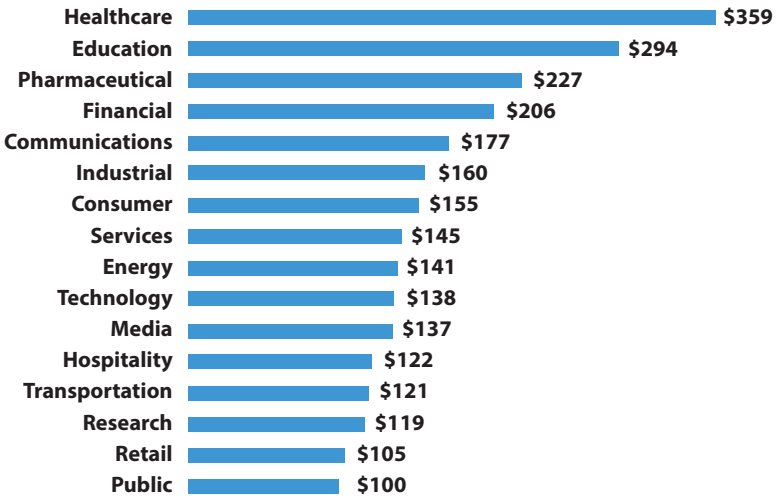
24025 Park Sorrento, Suite 405, Calabasas, CA 91302
Phone: 818-582-4952 | Email: solutions@prolifics.com
www.prolifics.com

The Rising Cost of a Data Breach

Over 300 companies surveyed in a worldwide study conducted by Ponemon Institute[i] reported the average cost of a single data breach increased 15 percent over the last year to $3.5 million. The average cost paid solely for each lost or stolen record containing sensitive and confidential information increased from $136 in 2013 to $145 in 2014. A single data breach could result in tens of thousands of records being exposed or compromised. These records are defined as "information that identifies the natural personal (individual) whose information has been lost or stolen," and could be anything from customer credit card information to health insurance records with physician and payment information. Organizations today are faced with a new reality—one in which they are presented with a growing number of security threats that are more intelligent and damaging than ever before.

Certain industries have higher data breach costs. This figure reports the per capita costs for the consolidated sample by industry classification. Heavily regulated industries such as healthcare, education, pharmaceutical, and financial services had a per capita data breach cost substantially above the overall mean of $145. Public sector organizations and retail companies had a per capita cost well below the overall mean value.

Per capita cost by industry classification.
Consolidated view (n=314)



Advanced persistent threats—targeted cyber-attacks designed to bypass firewalls and anti-malware programs—are also on the rise; on average, these can cost an organization as much as $9.4 million[ii] in brand equity alone.

Target faced severe criticism in 2013 when about 70 million customer credit and debit card information was compromised, resulting in more than $61 million in costs

Target Inc. fell victim to a highly-publicized data breach after criminals forced access into the retailer's system during the 2013 holiday shopping season[iii]. The credit and debit card information of roughly 70 million customers was compromised, as well as names, mailing addresses, phone numbers and email addresses. This incident also resulted in the resignation of the company's CEO. To date, it has been reported that Target has spent $61 million addressing the breach and also suffered a loss in customer sales, not to mention the pending lawsuits from banks and shareholders.

In a similar breach, TJX Companies, Inc. paid a $9.75 million consumer protection settlement with 41 states after hackers stole the credit card numbers of as many as 94 million customers in 2007. It was reported that hackers broke into the database with a telescoping wireless antenna while parked outside a Minnesota Marshalls. They intercepted payment information and decoded data from hand-held payment scanners. During the investigation, it was reported that the company was slow to adopt the stronger, upgraded Wi-Fi Protected Access (WPA) protocol and failed to meet security procedures mandated by the credit card industry[iv].

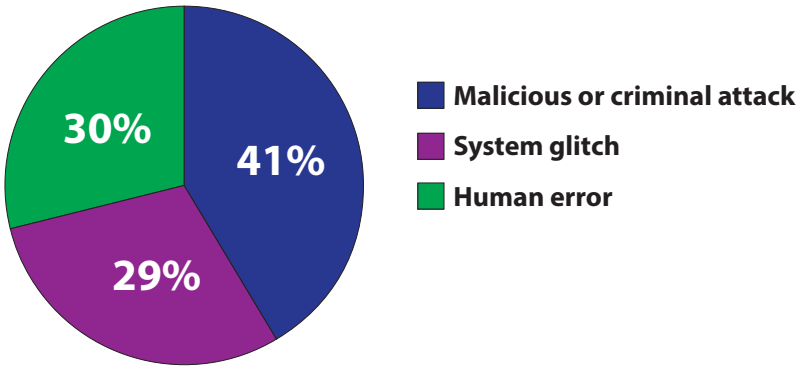
These cases are not isolated. In 2013, the Identity Theft Resource Center[v] received 614 reports of data breaches in the United States, a 30 percent increase over the total number of breaches tracked from the prior year. This data suggests that in today's climate, it's no longer a matter of whether or not a company will be breached; it's a matter of when.

The circumstances behind these incidents vary, from hackers to insider theft. Yet, in many cases, it is difficult to distinguish internal threats from external threats. Long gone are the days when employees sat at office desks and documented sensitive information on paper. Today, information is passed through email and other digital means and, as a result, the physical perimeter of a building is no longer a sufficient means of protection.

Data breaches in the United States have increased by 30% compared to the prior year

The best line of defense against these threats is a robust security strategy that works from the inside out. With maximum visibility into the identity of users with access to cyber networks, organizations can use real-time data to detect and resolve a cyber-threat before it becomes a full attack.

The root causes of data breach
Distribution of the benchmark sample by root cause of the data breach
Consolidated view (n=314)



Prolifics has worked with hundreds of fortune 1000 companies to implement their IT vision and has designed an identity intelligence solution that addresses its clients' greatest vulnerability—the lack of insight to exactly who is accessing networks and what they are doing. Built around IBM's security framework, Prolifics' identity intelligence solution focuses on the people within an organization by establishing rules and processes around the "who" of an event within its network. The multi-layered approach to implement both identity and access management, along with security intelligence, offers organizations the ability to more intelligently manage security risks in real time and ensure employees work more securely.

Stay Protected from Modern Threats with a Multilayer Security Approach

Perhaps the greatest advantage—and disadvantage—of the Internet is that anyone can access any data anywhere. From customers' credit card information to hospital patients' confidential records, data stored online is much more vulnerable to being intercepted. Ponemon reports[vi] that 42 percent of data breach incidents involve malicious or criminal attacks against an organization, and, on average, organizations in the United States rank highest in the number of exposed or compromised records—29,087—during a breach.

To avoid potential risks, organizations must grow their security models at the same rate as they grow their online presence. Too many companies have one foot in the modern digital world of ecommerce, and the other foot in the past with a security strategy that has not

changed since the advent of the Internet. Akin to the construction of a new state-of-the-art building without locks on the front door, organizations that move operations to the Internet, cloud, and mobile devices need to also align their security measures with these new methods of business and customer interaction.

While the majority of detected threats are external, the biggest economic impact on organizations—in terms of image, compliance, financials, and IT capital—comes from internal threats. In the majority of these cases the threat isn't rogue employees, but rather inadvertent inappropriate access.

According to Gartner Inc., about 90 percent of an organization's security budget is spent on perimeter control—network firewalls, intrusion protection devices, and other processes that close off the organization from the external threats. However, studies show that three-fourths of the breaches that cause real financial and security damage to an organization are internal actions from criminals who have penetrated the environment through someone within its trusted boundaries.

Even if an organization has locked the IT equivalent to every door, window, and hole in the roof, cybercriminals only need to find one point of entry, and will continue to try every door and window, computer connection, mobile device, and email, until they find a way to get in. It just takes one employee's click on a wrong email or link to introduce a virus that exposes the entire organization to theft and can cost the organization millions to recover. These breaches often happen in hours and days, but organizations typically won't discover the breach for weeks, months, or even years. This is partly due to the absence of the right set of forensic tools. Businesses are not watching what's going on closely or frequently enough.

Cloud, mobile, and social technologies have compounded these risks. Consider the large amount of data that is constantly transmitted across and within companies. Cloud and mobile technologies enable this data movement on production, customer relation, and access standpoints, but security and controls have not been implemented at the same pace. Firewalls add protection around networks, but what happens when a cybercriminal penetrates that wall? Vulnerabilities can take many forms: There could be an improperly set-up Wi-Fi network; or an employee lost his/her computer or smartphone; or there might be an employee at a company with ill-intent.

62%

of organizations have not aligned their information security strategy to their risk appetite or tolerance

source EY Building a better working world

A recent report by Trend Micro[vii] describes an ongoing worldwide attack that targets online banking and is designed to bypass SMS-based two-factor authentication systems used by banks. This malware tricks users into installing it onto smartphones through spear-phishing emails, which then allows attackers access to customers' bank accounts.

These kinds of attacks signal that the concept of perimeter security has faded, and every company should now assume that the criminals are already on the inside and therefore should treat all insiders as if they are the cyber threats by verifying each and every transaction.

In the last three to four years, the goals based on security threats and compliance requirements have changed exponentially. What was once just an IT issue is now a complex, multidepartment project that demands boardroom attention. Ernst & Young's latest annual Global Information Security Survey[viii] found that "although organizations have made strides in the right direction, there remains room for improvement. Many organizations are increasing investment in information security, yet many information security professionals continue to feel that their budgets are insufficient to address mounting cyber risks."

Of those surveyed[ix] , only 35 percent of organizations have their information security professional present to the board or members of the top governing structure quarterly. Yet, compliance should be driven by the business, instead of a sole reliance on IT. For example, a hospital must not only focus on its responsibility for making people well, but also on the fact that it is a custodian of their generated data. Protection of that data should be in multiple

layers to create the necessary defensive depth. Without proper protection and monitoring, critical data is readily accessible as soon as a hacker is on the internal network.

The immediacy and creativity of the threat landscape is also changing. Threats are planned creatively and delivered persistently. This is compounded by the explosion of means to access corporate systems, the growth of social media, bring-your-own-device, and mobile access. Ernst & Young's report found that 45 percent of respondents feel mobile computing has most changed their risk exposure, 32 percent cited social, and 25 percent cited the use of cloud computing.

While many organizations have improved their information security programs over the last 12 months, findings show[x] that leading organizations take improvement a step further with an established commitment from executives, adequate IT staffing, continuous monitoring and improvement of security plans, and a security strategy that extends traditional IT controls.

Typical IT Security Controls:

1. *Corrective: Mitigate or lessen the effects of the threat being manifested*
2. *Detective: Identify that a threat has landed in the system and what it's doing*
3. *Preventive: Identity and access management to prevent the threat from coming in contact with the system*
4. *Deterrent: Discourage individuals from intentionally violating information security policies or procedures*

Extend Traditional Controls of Security Information and Event Management

Today, most organizations have some form of a security information and event management (SIEM) system that creates logs when employee-related events occur. There are thousands of types of security controls that produce logs, including badge systems, physical controls, assess management systems, identity provisioning systems that onboard and offboard employees, network access events both within the system and communications to the outside, integration with outside business partners, and federated identity.

The root of security lies in understanding who has access to what, and where, and when, and whether they are entitled to have that access. Logs store the data, which is then used to identify and address security threats. These are critical when an organization undergoes a security audit and must prove, for compliance reasons, that it only allows the right people to access the right data at the right time, in terms of entitlement. This type of log-based security system centers on preventive control—organizations can either close down or open access based on entitlements.

In response to the changing security landscape, now organizations must identify threats in real time, rather than wait for the next audit or access report to learn if there was inappropriate access. To know about threats in real time transforms the security process from preventive to protective control. Real-time control allows organizations to use those logs not as backward audit-type events, but as real-time alerting events. The concept of identity management is at the core of this capability.

With identity management, organizations can assert control over access to sensitive data, how it monitors that behavior, and how it responds to violations. The main goal for identity management systems is operational: to automate a permissions process that had traditionally been performed manually. For instance, when a new employee joins an organization, there is a process that is performed to provide that new employee access to the applications and IT resources needed. This identity provisioning can be an operational headache unless the process is automated. Manual and uncomprehensive audit trails are tedious work, and if held up or done incorrectly, organizations can run into trouble meeting compliance codes.

These traditional SIEM networks log what event happened, where it happened, and when it happened. But that's where it falls short. While it documents the name of the account that initiated the event, it fails to capture any of the context of who that person is. For example, a traditional SIEM will document that Jay Smith at Company X logged into the organization's system—but who is Jay Smith? What privileges does he have? What should he be doing? What shouldn't he be doing? Was he fired yesterday? Has his name been stolen? Did he log in from a typical or abnormal location?

Similar to a credit card company that tracks the purchasing habits of its customers—if you buy a bagel with your credit card that can be considered normal behavior, but if you use your credit card to buy a Ferrari, the credit card company will likely consider that a strange behavior, or if you try to buy a Ferrari in Kazakhstan, that's a behavior that likely will be seen as inappropriate—the key to identifying appropriate behavior lies in knowing the customer's buying patterns: to know the actor behind the actions.

In security, this context must be integrated with the traditional SIEM network activity, and more complex business rules must be established in order to systematically track the events. If the SIEM is able to consume the identity provisioning logs from an identity management system, it's able to understand more about the "who" of an event—who the person is, what their role is, and whether or not they actually have the permissions and entitlements to access the data.

Prolifics' Identity Intelligence Solution

Prolifics—a leader in preventive controls for 10 years—is at the forefront of access governance, which answers this question of context. Prolifics' identity intelligence solution serves as a custom add-on to IBM Security QRadar, one of the leading SIEM technologies on the market. While IBM Security QRadar has basic integration with the identity stack to allow the logs from the identity and access management systems to see identity logs, it lacks the context component to specify the exact violations to detect based on an individual's prior actions.

The Prolifics' Identity Intelligence with QRadar adds this layer of security intelligence onto IBM's mature identify management platform and extends the integration of traditional SIEM and identity management to better govern the activities of users, understand their behaviors in real time, and analyze activities as patterns. The ability to integrate the who, what, when, where and how of employee behavior into the broader security infrastructure gives organizations a real-time view into their threats from the insider environment.

Using the development language of the SIEM, Prolifics custom built the business rules and mappings that allow IBM Security QRadar to interpret dozens of the most common identity-related violations. For instance, if the CFO of a company logs into the financial data system at 5:30 p.m. on a Friday and is transmitting sensitive accounting files to an outside repository, that event is not necessarily concerning because that CFO has permission to access the data. However, an SIEM with identity intelligence understands the context of the network flow and network access events and has, over time, built a profile about the user from past activity. That profile shows that the CFO always logs in from one of four IP addresses—two are at the office and the other two are the CFO's home and vacation home—and all four are located in California. Therefore, if this Friday afternoon activity is being tracked to an IP address in Oklahoma, suddenly that event is no longer innocent and flags are raised.

Profiles consist of rules built in the SIEM and are based on the organization's data and policy sensitivities. These profiles tell the system whether an event is concerning or not. Then, depending on the level of risk, the organization can determine whether to escalate the event to various types of mitigating actions immediately, such as shutting down the IP address, or if an initial notification is appropriate. Notifications can be sent to the user accessing the sensitive files. For example, these notifications could request the user to stop the activity or answer a security question to prove the user is authentic. All these things can be adjusted based on the sensitivity of the access and event.

This addition of identity intelligence to IBM's SIEM is a custom integration effort that requires new code, which can be easily adjusted to any organization's specific policies or entitlements. Prolifics has templates of mitigating actions that depend on the organization's specific risk profile and what actions are required. Organizations gain deeper insight into the identity of employees and partners who come into contact with internal data and are better poised to

Top 7 Most Common Security Rules:

Prolifics' identity intelligence solution allows for specific rules to be added to standard SIEM networks.

Examples of these rules include the following:

1. *List any and all activities of people no longer employed (for example, terminated users), or whose accounts weren't properly terminated, or were shared*
2. *List activities of contractors/consultants related to production systems*
3. *List activities of administration personnel (are they doing any unusual activities, for example, creating, then deleting accounts)*
4. *List activities of executive personnel (watching for identity theft)*
5. *List "unusual" activities (for example, large data transfers, weekend or evening activity)*
6. *List activities of particular groups who have access to high-value data (finance, HR, legal)*
7. *List activities of "outside" personnel (supply chain, contractors)*

properly manage risk, and also have access to Prolifics' expert group of security professionals to build and analyze business rules and monitor activities and changes, putting them in a prime position to identify and address security threats.

In today's evolved cyber-criminal environment, the quicker threats and breaches are discovered, the less costly they are for organizations. Ponemon's 2013 study on the cost of cyber crimes showed a direct correlation between the time it takes to contain an attack and the cost. The report also found that companies that monitor cyber crime with security intelligence technologies realized an average cost savings of nearly $4 million when compared to companies not deploying security intelligence technologies.

As public security breaches make more headlines, this issue is making its way to the top of boardroom agendas. A major national insurance company, for instance, had recently planned to roll out a security solution over 18 months, however in light of the slew of recent security breaches, the Board of Directors intervened and gave the team five months to assess the market, buy a tool, and get it up and running. After spending $1 million on software, they brought Prolifics on to design the system and within a few weeks, Prolifics had the first elements of the operational system live, with ongoing work over the next few months to complete the system and implement all the customizations.

Prolifics' experts not only take care of the architecture and design, but also the implementation and monitoring. The company's security professionals manage the identity intelligence solution twenty-four hours a day, seven days a week in both the United States and in India, and alerts clients as events are detected that go against the established business rules. Prolifics' managed services employees monitor the security directly, however system stability—hardware and software—is monitored automatically. This allows organizations to maintain control of its systems while benefiting from not actually needing to find staff with the appropriate high skill level and knowledge to manage the systems.

The Path Forward

The key to rock-solid security is risk management. With so much technology available, organizations are often more susceptible to vulnerabilities and breaches if they look only at entry points and not at access levels and activities as well. Products are available to protect systems; however in most cases, because it hasn't been part of IT culture and business culture to date, the proper security platform isn't built in to the system from the beginning.

The biggest cost differentiator when a breach occurs is the time it takes to detect and resolve the incident. Based on feedback Gartner Inc. has received, in addition to the benefits of overcoming staffing shortages and skill deficiencies, organizations cite the importance of time-to-value and resolving conflicts over duplicative identity and assess management implementations. Many of Prolifics largest clients monitor two billion events a day. IT breaches typically are the result of a series or chain of events. Many events will raise no flags, however if a monitoring system is simply logging each event separately, when one event is flagged, that chain goes undetected. This increases the time it takes to resolve the breach. Prolifics' identity solution brings these events together and builds profiles for each user or IP address, which makes it easier to find out who is behind a breach and stop it.

As technology continues to develop and wearable devices become more mainstream, a completely new treasure-trove of information will be available for cyber criminals to try to gain access. It's a five-year cycle of growth and opportunity, but if security doesn't evolve at the same pace there is an imbalance between the convenience of access and the cost of too few controls in place. Whether the threat is a malicious insider, criminal outsider, or a case of identity theft, the presence of an integrated identity intelligence solution within SIEM will detect the "who" behind the "what" of the event and allow for the consequent opportunity to act quickly and lower both the financial and reputational costs of the breach.

More Information

About Prolifics

Prolifics, an IBM Premier Business Partner and multi-award winner for technical excellence, creates competitive advantage by delivering customized, end-to-end Business Process Management, Integration, Mobile, Big Data and Cloud solutions that achieve business success. For over 35 years, our technology expertise, industry-specific insight and certified technology accelerators have transformed organizations around the world by solving complex IT challenges. Our expert services include architectural advisement, design, development, and deployment of tailored solutions that empower businesses around the world to create flexible business services and build agility into their organizations.

For more information about Prolifics, visit www.prolifics.com.

Contact Information

Phone: 1-800-458-3313
Phone: 212-267-7722
Email: solutions@prolifics.com

About the Author:

Natalie Miller is the Editor of *Insights Magazine*, www.insightsmagazineonline.com, a digital publication that provides comprehensive coverage of IBM solutions for analytics, mobile, social business, and cloud, plus solution-specific content on WebSphere and other IBM software brands. Natalie is a journalist with nearly 10 years of field experience and has written countless case studies and features on technology, for both strategic and technical audiences.

References

[i]http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis
[ii]http://securityintelligence.com/media/2014-ponemon-study-economic-impact-advanced-persistent-threats-apts/#.U9pu5fldU4d
[iii]https://corporate.target.com/about/payment-card-issue.aspx
[iv]http://www.consumeraffairs.com/tj-maxx-data-breach
[v]http://www.idtheftcenter.org/ITRC-Surveys-Studies/2013-data-breaches.html
[vi]http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis
[vii]http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-finding-holes-operation-emmental.pdf
[viii]http://www.ey.com/Publication/vwLUAssets/EY_-_2013_Global_Information_Security_Survey/$FILE/EY-GISS-Under-cyber-attack.pdf
[ix]http://www.ey.com/Publication/vwLUAssets/EY_-_2013_Global_Information_Security_Survey/$FILE/EY-GISS-Under-cyber-attack.pdf
[x]http://www.ey.com/Publication/vwLUAssets/EY_-_2013_Global_Information_Security_Survey/$FILE/EY-GISS-Under-cyber-attack.pdf