Security for a Faster World

In this issue:

Issue 3, 2013

Contents…

Security for a Faster World

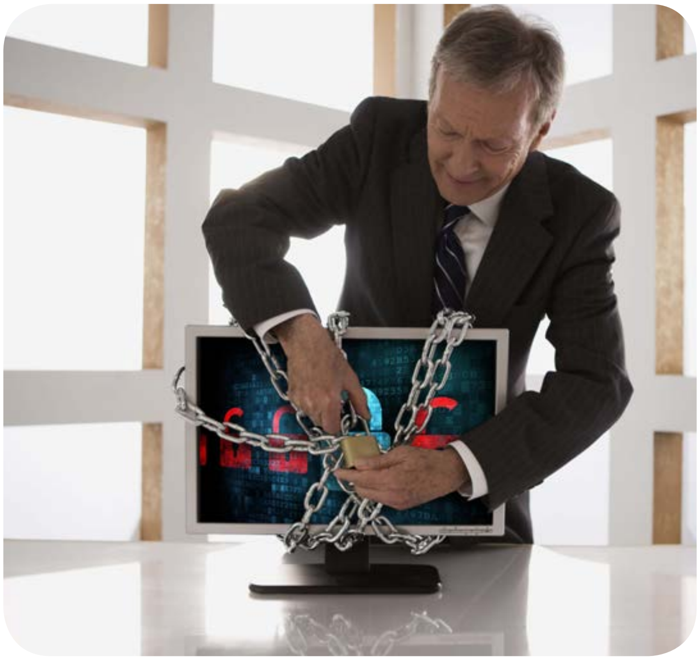
Contributors: Amy Newman, Paul Rubens, and Michael Pastore.

How Secure Are You?

By Amy Newman

Cyber crime. The very word sets many CIOs' hearts racing. Although far from a new threat, cyber crime is getting increasingly sophisticated, often nipping at the heels or surpassing the security of enterprises. Security tools and programs are constantly evolving to meet the new challenges, and security planning is no longer just an annual event. As attack methods change, so too must defense strategies if they are to stay ahead of the curve.

As cyber crime becomes increasingly advanced, it is also becoming pervasive and costly. The 2012 Cost of Cyber Crime survey[1] conducted by the Ponemon Institute and sponsored by HP examined 56 companies across all industry verticals to get a picture of the impact and costs of cyber crime. Companies across the survey base experienced an average of 102 successful attacks a week, an increase of nearly 42 percent over the 72 attacks per week experienced in 2011. Complicating matters was the fact that the attacks were stealthier than in the past, which led to longer remediation times. The study found it took an average of 24 days to contain a cyber attack, up from 18 days in 2011.



These factors contributed to the rise in the average annual cost of cyber crime, which increased by 6 percent to $8.9 million in 2012.[2]

While cyber attacks are growing and becoming more costly, the 2013 Global State of Information Security Survey conducted by PwC, *CIO Magazine, and CSO Magazine* reveals that most companies are confident in their existing security program. How can this be?

It is not easy to evaluate how secure your enterprise actually is. Nor is it easy to determine how secure it should be and figure out the necessary steps to get there. Perhaps an objective view is needed.

The Security Maturity model, developed by Cindy Blake at HP, makes it easier to answer these questions, offering executives a clear reference point for enterprise security and subsequent steps in the trajectory.

The Security Maturity model, shown in Figure 1, asks enterprises to look at what steps they are taking to mitigate risk factors while improving their agility as they prevent, detect, and remediate attacks. Where an enterprise is on the continuum determines the maturity of its IT security management. While not every enterprise will need predictive capabilities, most will need to go beyond basic defensive protections. And all enterprises can benefit from a more integrated approach. An offensive strategy can protect against more sophisticated threats and even against undetected breaches that may have occurred long ago.

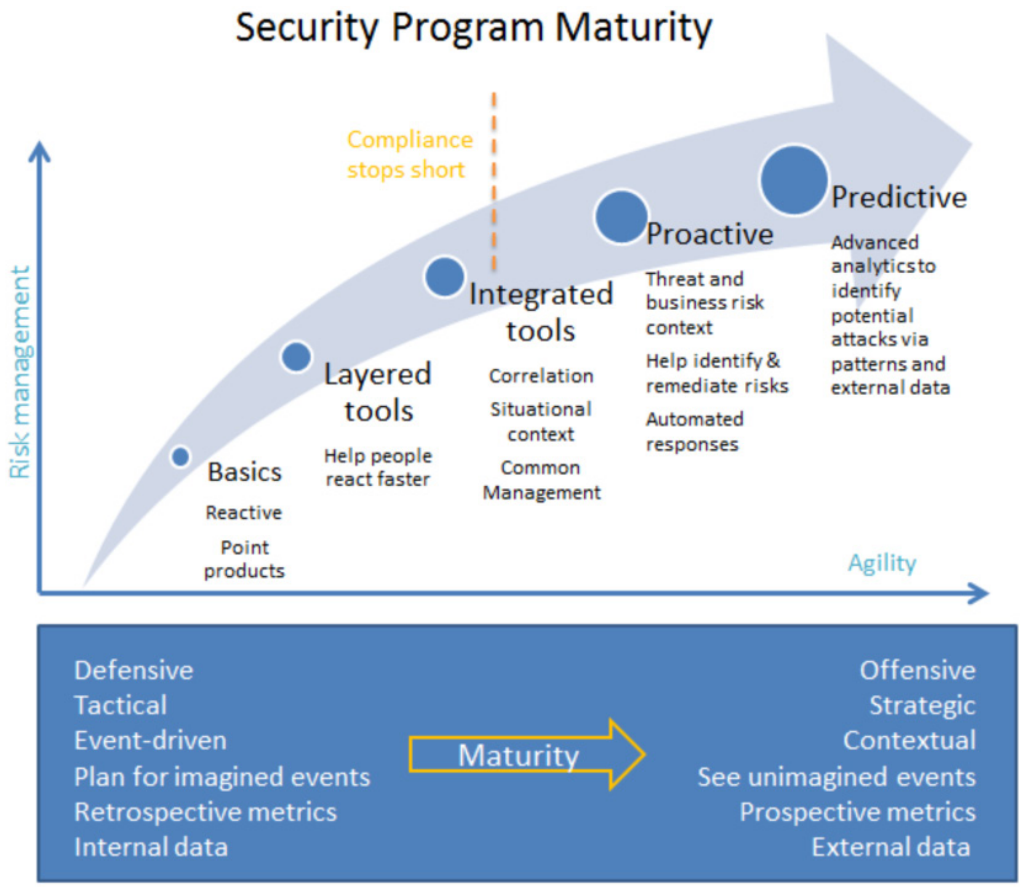


Figure 1: *The Security Maturity model enables enterprises to look at the steps they are taking to mitigate factors and offers ways to improve agility.*

States of Enterprise Readiness

Basic Tools: As a basic defense, perimeter protection, such as intrusion detection, can identify and report a potential security attack. HP was the first to go a step further, offering intrusion prevention, which not only identifies suspicious network activity but also blocks malicious executables and files, more quickly stopping potential damage.

As fundamental protection, intrusion prevention is one of the most efficient methods of security policy deployment and is widely adopted. The recent Global State of Information Security Survey found that 50 percent of its 9,300 respondents worldwide have intrusion protection systems in place while 78 percent of the security leaders employ it.[3]

HP TippingPoint Next Generation Intrusion Prevention System is relatively easy to deploy. It does not require network reconfiguration and has very low latency, making it nearly invisible to the user. And, for even greater protection, it regularly applies threat intelligence to protect against dynamic new vulnerabilities.

These basic defensive tools are critical, but for many enterprises they are not enough. As the Ponemon report notes, new threats can get around even the most sophisticated network defense, and malicious exploits are often implanted years before they are discovered. Using multiple tools to detect and prevent a variety of attacks affords even greater protection.

Layered Tools: A layered approach is typically called "defense in depth." It uses multiple tools and policies to safeguard various attack vectors including system, network, and application levels as well as data transmissions. A layered approach enables faster reaction against a broader set of threats. For some enterprises, even a few minutes of interrupted service can have a significant impact, whether in the form of lost revenue or even, for example in the case of emergency services, lost lives.

Often data encryption is added to intrusion prevention so that if network security fails, sensitive data remains protected. In fact, encryption is required by many regulatory agencies. If data is breached, encryption will prevent it from being useful to the attacker. It is important to encrypt data both at rest and in motion to ensure complete coverage. Tools like those offered by HP Atalla can enable cryptographic processing and simplify encryption key management.

As another layer, security events may be captured and logged for further review. Log management solutions facilitate the log collection, archival, reporting, and investigation capabilities that regulatory compliance typically requires; they are also considered a general security best practice. The challenge for using these security event logs is that every device may send data in its own unique format, making it tedious to interpret the compendium of data. HP ArcSight can translate disparate data feeds into a common format to simplify and automate review and analysis, surfacing issues more quickly.

While layered tools provide a tremendous amount of protection, for enterprises focused on compliance requirements, they are a bit like looking in your rear-view mirror. Compliance alone tends to focus on the lowest common denominator—what can the majority of enterprises subject to the controls feasibly do? If compliance were a high bar, a majority would fail regulatory audits. Cyber attackers are infinitely more advanced than average security controls. For this reason, most organizations will need to look beyond point products offered by individual security tools.

Integrated Tools: The more security-mature enterprise looks to correlation, situational context, and integration to provide the best insight and protection. At the same time, common management may afford efficiencies for security operations.

Understanding which security events are troublesome and which are benign can be daunting. By correlating seemingly unrelated events in real time, HP ArcSight can quickly bring critical concerns to the surface. Automating much of the analysis and reporting can make security and compliance management more effective and efficient.

Even greater context can be applied to this correlation and analysis by including data about the user's identity and authorizations, reputations of network traffic sites, and IT system performance. Users attempting to access sites for which their role is not authorized can trigger a security event. Traffic to or from sites with known bad reputations can trigger the need to quickly block the traffic. And servers or routers with atypical loads can suggest denial-of-service attacks when correlated with other security events. Tools that work in an integrated manner can offer far greater protection than individual point products.

Integrated tools that can quickly connect the dots between threats and business risk can improve your agility—your ability to identify, stop, remediate and prevent security breaches. HP EnterpriseView does just that, connecting IT assets to the business functions they support, and then adding the perspective of compliance and composite risk using actual security events in near real time. By enabling meaningful conversations around business priorities and security investments, this can position the enterprise for a more proactive approach.

Proactive Tools: Proactive tools are designed to catch potential threats with the most business risk. Examples of proactive approaches include application vulnerability assessments, incorporation of threat intelligence, and IT governance, risk and compliance (IT GRC) management.

Applications are now one of the most frequent targets for attacks, IDC reported in its briefing at the RSA conference (February 2012). Applications that are most critical to the business should certainly be assessed for security vulnerabilities, but even those less critical can become the weakest link and offer an easy entrance for potential attackers. HP Fortify can scan applications to identify vulnerabilities, whether the application is custom developed or from a third party, and whether it is in production or development. Although changes

"Predictive tools go beyond traditional security approaches to look for threats outside the organization."

to development code are less costly than modifying code in production, it remains important to test legacy applications not developed with cyber security in mind.

Threat intelligence can provide early identification of vulnerabilities, especially for popular targets, like Microsoft products. HP DVLabs identifies more vulnerabilities than HP's top 10 competitors in this space combined.[4] Subscribers to HP DVLabs have been able to block vulnerabilities well before the vendor issues a patch to the public.

IT GRC tools can quickly focus action on threats with business risk. By using a simple heat map, HP EnterpriseView quickly highlights areas needing the most attention, based not only on current security events and activities, but also on relevance to the business.

To truly thwart new and evolving adversaries, even this level of protection is not enough. Predictive tools go beyond traditional security approaches to look for threats outside the organization.

Predictive Tools: Predictive tools use advanced analytics to identify potential attacks via patterns in external data. This approach protects against unimagined, and thus unanticipated, threats—before they ever appear as a security event in traditional security systems. With these tools, enterprises take an offensive strategy.

Consider the ability to identify disgruntled employees before they can inflict damage to the brand image or to the bottom line. Sophisticated hackers have become specialists in their trade, with online exchanges in which to market their exploits. What if you could stop them during their planning stages, before traditional security programs would have recognized a potential threat? Predictive security can be quite powerful, particularly for industries most targeted, such as critical infrastructure and financial services or those with the most sensitive data, such as healthcare.

While predictive security offers the most advanced protection, it should not be used alone. Without a solid foundation of basic security, layered tools, and the scaffolding of integrated and proactive capabilities, relying on predictive tools alone affords little protection once an attacker strikes.

Where Are You on the Curve?

How secure are you? How much security is enough? Although it is important to meet compliance requirements and secure the perimeter, remember that threats are constantly evolving. As the adversaries become more sophisticated, so must your capabilities.

And before deciding where on the curve you need to be, it is important to determine where you are. In addition to the tools mentioned in this article, what processes do you have in place, and how mature is your overall security and compliance program?

For more information on the HP Enterprise Security tools mentioned, go to www.hp.com/go/sirm. ■

[1] *http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf*

[2] *http://www.esecurityplanet.com/trends/cyber-crime-is-cost-going-up.html*

[3] *http://www.pwc.com/gx/en/consulting-services/information-security-survey/giss.jhtml?region=&industry=*

[4] *Frost & Sullivan, Analysis of the Global Public Vulnerability Research Market in CY 2011, April 2012*

5 Security Questions Every CIO Should Be Able to Answer

By Paul Rubens

Profitability and growth are two signs that a business is successful. To achieve these, companies must be well managed, agile, and innovative. But they also need to be secure, and that means protecting their intellectual property, business services and data, and the privacy of their customers.

Enterprise security is becoming increasingly complex, and the CIO's job is becoming harder for two principal reasons. First, it's no longer enough to secure the business perimeter and keep hackers off the corporate network. That's because new IT trends like cloud computing and mobility mean there is no clearly defined perimeter to secure.

Second, the security threats enterprises face are growing — in frequency, in type, and in complexity. Organized crime gangs, hacktivist groups, and even foreign government-backed experts pose a far greater threat today than the opportunistic amateur hackers of the past. There is also the problem of identifying threats that originate inside the organization — these include malicious employees or contractors and industrial spies along with well-meaning employees who inadvertently compromise security.

The bottom line is that these threats introduce security risks, and since they can't be eliminated completely, they must be managed, just like financial or physical asset risks. Investment in enterprise security is, in a sense, a form of insurance. It can help reduce the likelihood of a security breach, minimize the impact if one does occur, and allow for faster recovery. Like any insurance, it comes at a price, but the alternative is a greater risk of incurring costs or damaging brand reputation.

To properly manage such risks, CIOs must have answers for five critical questions.

Question 1: How are we ensuring compliance with privacy laws and other regulations here and abroad?

Taking steps to keep confidential customer data secure is considered so important that privacy laws set out legal requirements with which enterprises are required to comply. Failure to do so can expose the company, its managers, directors and officers to fines and — in some cases — imprisonment. That means any CIO responsible for non-compliance is putting his career and freedom on the line.

A major problem for CIOs is that there are hundreds of different local, state, federal, and international laws that a business may be subject to, depending on the industries and business sectors in which it operates. This affects all businesses, but it's a more important issue for any company that holds the financial records, credit card numbers, or medical records of its customers.

Non-compliance can be caused by a failure to understand which privacy laws govern a company's activities or by failing to implement and enforce effective policies and procedures to ensure compliance. The financial risks to a company due to non-compliance vary according to the laws concerned. To give an idea of potential exposure, breaches of HIPAA can lead to fines of up to $250,000. Employees responsible for breaching regulations for commercial advantage, personal gain, or malicious harm may also face up to 10 years in prison. Less quantifiable, but arguably more costly to an organization, is the loss of reputation and future business that may result from private information being stolen due to non-compliance.

The key way to ensure compliance is to conduct regular compliance audits that establish which regulations the company is subject to and ensure that all appropriate policies, controls, and procedures are implemented and adhered to. Tools, such as HP EnterpriseView, that simplify compliance management using real-time security events can help avoid surprises.

Question 2: How are we protecting ourselves in a world dominated by mobile devices and free Wi-Fi?

Employee use of tablets and smartphones — both corporate and employee owned — has exploded over the past few years, adding millions of new mobile devices to the fleets of laptops already used in many organizations.

While mobile devices enable more flexible working practices and can increase productivity, they also provide a security challenge to CIOs because they can't be managed and monitored as easily as the traditional desktop PCs sitting within the corporate perimeter.

They introduce "device risk." For example, if a device is lost or stolen, all the data it contains could be compromised, along with any systems on the corporate network it is able to access. And, without adequate protection, employees can unwittingly introduce malware into an organization when they connect a mobile device to the corporate network.

The most effective way for companies to protect themselves against device risks is to implement a mobile device management system. These bring mobile devices under enterprise control by enforcing security policies, such as requiring the contents be encrypted and requiring a long password to unlock the device. They can also lock or remotely wipe lost or stolen devices. Another layer would be identity management, which ensures only authorized users have access to the data.

Mobile devices also introduce "application risk": Malicious apps on a mobile device may access

"A major problem for CIOs is that there are hundreds of different local, state, federal, and international laws that a business may be subject to, depending on the industries and business sectors in which it operates."

sensitive data on the device and send it to third parties. Applications designed to provide customers or staff access to corporate systems, but that have weaknesses like poorly implemented cryptography or poor authentication may be exploited by hackers to compromise corporate security.

Application risks can be mitigated by testing mobile applications for vulnerabilities—both your own and third-party apps. Applications can be vetted using security solutions, such as HP Fortify, designed to detect, fix, or prevent security vulnerabilities.

Question 3: How do we ensure cloud applications being used are secure?

When a company runs applications in the cloud, the security implications are very different from when the same applications are run in a corporate data center. Security responsibilities of the cloud provider and customer can vary greatly. Cloud providers are generally responsible for the underlying cloud platform, which includes the virtualization layer as well as the physical security of the servers and data center that houses them. The security of cloud applications offered by a cloud provider (software as a service, in other words) may also be the responsibility of the cloud provider. However, customers should check indemnity clauses carefully.

It is the customer's responsibility to ensure that the cloud provider's security measures and claims are effective and credible. That could involve examining its policies and procedures, ensuring relevant certifications have been obtained, or even assessing proprietary source code.

Customers are also frequently responsible for data encryption to ensure the security of any data stored by the cloud service provider. This can be achieved by controlling and managing encryption keys and carrying out encryption at a gateway to the cloud provider.

However, before this can begin to be addressed, the customer must know what cloud applications its employees are using. This is as much a policy issue as a technology issue. It's particularly important to establish clear rules about employee use of consumer cloud applications, such as DropBox, Google Drive, and Carbonite. These offerings rarely deliver enterprise grade security, yet they allow employees to store data — including confidential corporate information — outside of the corporate network, beyond the reaches of internal security measures. This could affect compliance with privacy regulations and be costly, should a data breach occur. The use of consumer cloud applications can be disallowed with measures such as blocking the domains, IP ranges or data types with a corporate firewall.

The most effective way to deal with the risks of cloud applications is to run them in a private cloud in a data center over which an organization has complete control. This is not always feasible. Enterprises thinking of running applications in external clouds should first consider a thorough analysis of the cloud provider's security measures.

Question 4: How are we defending ourselves from internal threats?

Internal threats include malicious employees or ex-employees — often IT staff — who use their privileged position in an organization to access, destroy or steal data, or cause damage. But loyal employees can unwittingly pose an internal threat to an organization as well. They might, for example, provide passwords or other authentication credentials to a hacker, perhaps through a social engineering attack or phishing scam. They may also inadvertently download a malicious application that provides a hacker with access to computer systems, or take data home on a USB stick, where it is outside the protection of any corporate security systems.

All of these internal threats pose the risk that an organization loses control of confidential information or that malicious outsiders gain access to the corporate network and internal systems, bypassing existing security measures. Reputation data and threat intelligence are helpful to identify communications with known bad actors and bad addresses.

In addition, many organizations monitor employee computer usage to detect when an employee's usage patterns change, as this may indicate a malicious or disgruntled employee. Systems should also be in place to cancel an employee's network access and passwords when he leaves the company to prevent credentials from being used in a revenge attack. To be even more proactive, Big Data tools and advanced analytics can be used to look for potential threats externally, in social media communities. By looking for patterns and sentiments across a broad range of sources external to the organization, it is possible to identify threats not typically found via traditional security defenses. Ponemon reports that the average malicious breach affords the attacker access for almost a year before the breach is discovered. Hence, early detection can be key to successfully protecting company assets and intellectual property.

Question 5: How do we know if our security investments protect our most critical business functions?

No security infrastructure can provide 100 percent security, and that's why investments in security are about risk management. Hence, organizations must invest in areas where the risks to the business are the most significant, bringing them down to acceptable levels. Like any investment, security spending needs to be evaluated according to the likely return (in terms of reduced risk) that it will produce, and budgets allocated accordingly.

Understanding composite risk to your most important business assets and functions is key. Composite risk is made up of:

- Real-time risks—What risks or threats have actually manifested on my network?
- Vulnerability risks—How do I aggregate risk scores as I roll up my IT asset hierarchy to business functions?
- Compliance risks—How does configuration and policy drift factor add to risk?
- Intrinsic risks—How mature are the people and processes around my controls?
- Extrinsic risks—How do external factors (like earthquakes) factor into overall risk?

Tools, like HP EnterpriseView, which continuously manage this composite risk, are far better protection than those that afford only a snapshot with a reporting dashboard.

Enterprises should look holistically at the business. They should know which business functions are most important and which IT assets support them. Then, they must continuously assess the composite, real-time risk of those areas to determine how security spending should be allocated and risks mitigated.

Conclusion

The threats that enterprises face are growing, so the security measures implemented must evolve to mitigate new risks as they emerge. It's a continuous process, and if you fall behind, the consequences can be very serious indeed. Having a security partner like HP can make this evolution easier.

A security assessment carried out by independent experts is the first step in this ongoing relationship. Much like seeking out a third party to assess your insurance coverage, assessing your security and risk management program provides a necessary level of protection—particularly if you are unsure of answers to these questions. An HP Security Assessment will analyze your entire business—or a specific area of concern—and identify any threats your organization may have overlooked. It can quantify the risks that these threats pose, and outline, prioritize, and justify the various steps needed to mitigate and manage them.

For more information on powerful security technology and tailored services, visit HP's Integrated Security Solution page to learn more. ■

Time to Change the Security Game

By Michael Pastore

Regardless of what is being secured — electronic data, physical assets or currency — security efforts tend to focus on the perimeter. It's always been that way. Even before electronic data and hacking existed, those with something worth protecting put it inside a vault, dug a moat, or built a gate.

It's no surprise, then, that with the advent of information technology the approach to IT security followed roughly the same model: Build a wall around what you need to protect to keep it safe from those who want to take it. And over the years, as attacks grew more sophisticated and persistent, the popular approach was to build the walls higher, build the gates stronger, and restrict access to what needs protecting.

It's hard to blame those tasked with IT security for this paradigm. After all, they're involved in a cat-and-mouse game that goes back decades, trying to keep up with the latest threats, patch the latest vulnerabilities and secure data that freely roams beyond the network on mobile devices of all shapes and sizes.

This perimeter approach to security isn't always effective, as demonstrated by countless data breaches and online attacks. It's time to take a step back and ask if this approach is working. Here are some numbers from the 2012 Cost of Cyber Crime Study from the Ponemon Institute from October 2012 that indicate it isn't.

- Five times more security spend is focused on keeping the bad guys out than on finding them once they're in, blocking their efforts to access data, and preventing data leakage.

- Ninety percent of the companies polled by the Ponemon Institute expect to be compromised in the next 12 months.

- Once an attacker is in, the average time to detect the breach is 416 days.

What these numbers tell us is that businesses are throwing money at perimeter protection they don't expect will work to the detriment of security inside the perimeter.

An Alternative Approach

This is a bitter pill to swallow for many IT security professionals schooled in the old approach, but in today's environment you need to assume—and even expect—attackers will get in. IT security investments need to shift beyond perimeter security to disrupt hackers as they research how they can attack an enterprise, discover and capture sensitive data, and extract data after the fact.

Enterprise security vendors like HP are developing techniques that use what they know about today's attackers to create a more effective response. They know that attackers have developed an entire ecosystem of specialization where some focus on research while others might focus on exfiltration. They use vast online markets to exchange their results in loose circles of cooperation. One attacker may offer personal details about 50 executives, for example, which is valuable for use in spear-phishing attacks. Another may offer credit card data. Figure 1 shows how an ecosystem of specialists is developing around each element of an attack.

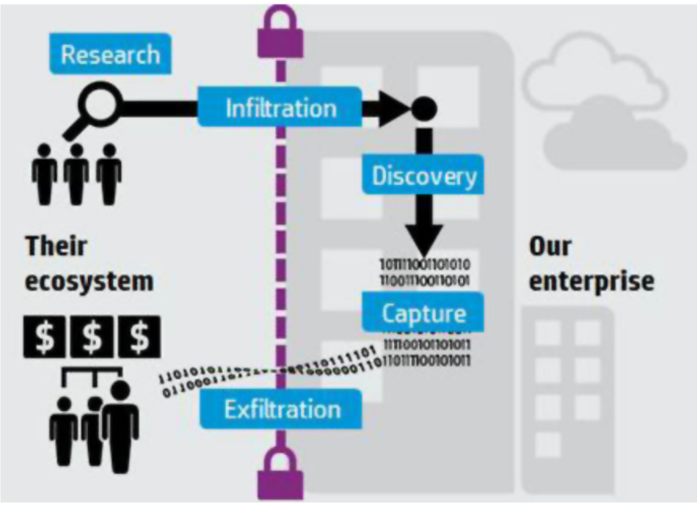


Figure 1: *Cybercriminals are developing an ecosystem where different players specialize in different aspects of an attack.*

Source: Ponemon Report

To protect assets and intellectual property, IT security needs an approach that organizes its capabilities to disrupt the attackers' ecosystem. Intrusion prevention can, of course, be employed to block access. But for those breaches that inevitably occur, enterprises must also focus on finding the intruder, protecting sensitive data and intellectual property, and quickly mitigating any damage.

As Figure 2 illustrates, a different approach to security is needed. Tools for the new security game must include context of meaning, geography, identity, and reputation, along with the ability to correlate seemingly unrelated events within this context for superior insight and protection.

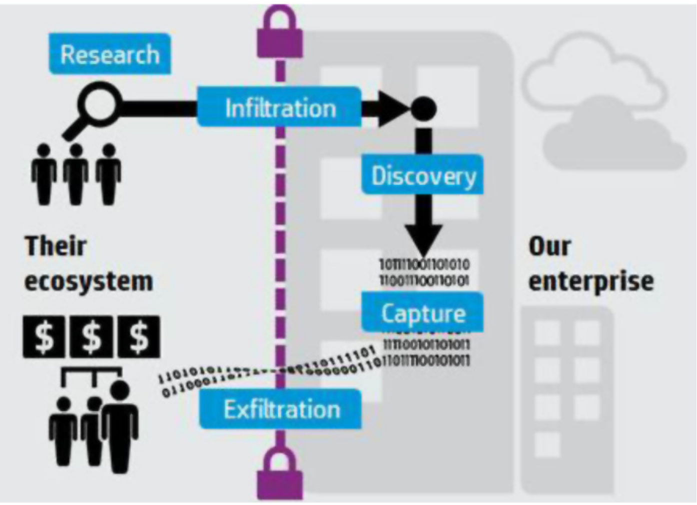


Figure 2: *A different approach to security.*

Powered By Research and Intelligence

The new paradigm for IT security less resembles a plan to keep attackers out (as traditionally is the case) and more closely resembles the tactics used to disrupt military operations. Like any successful military operation, this approach needs to be based on intelligence gathering and research.

HP has industry-leading security research via DV Labs, a research organization focused on vulnerability discover and analysis. DV Labs disclosed more verified vulnerabilities than the eight closest competitors combined, according to the April 2012 Frost & Sullivan report, "Analysis of the Global Public Vulnerability Research Market in CY 2011." In 2012, research from DV Labs was integrated with HP ArcSight, to create HP Reputation Security Monitor (RepSM), which is used to protect against advanced threats. This reputation data enhances the identification of peer-to-peer network use and improves detection of potential spear phishing and spam floods, while also recognizing patterns over time, such as those indicative of reconnaissance scans and abnormal activity levels.

At the 2013 RSA Conference, HP unveiled its HP Security Research (HPSR) organization, a new group that is charged with providing actionable security intelligence through published reports, threat briefings, and enhancements to the HP security product portfolio.

For HP, HPSR is taking the lead on the company's security research agenda, leveraging existing HP security research groups, including HP DVLabs and HP Fortify Software Security Research, which is focused on developing software security practices. HPSR is also managing the Zero Day Initiative (ZDI), which focuses on identifying software flaws that have led to cyberattacks and security breaches.

Taking Security Intelligence to the Next Level

Harnessing the power of analytics is nothing new for today's enterprise IT organizations. They are accustomed to using software to help sift through large quantities of data. They are mining Big Data to find new insights among the data generated by mobile devices, social networks, and more to give them a competitive advantage. The same practice can be put to work for security — analyzing vast quantities of data to find the type of clues and irregularities that could signal an attack.

Businesses can make the most of their investments in Big Data by harnessing the power of advanced analytics and aiming it at enterprise security intelligence. Products like Autonomy's Intelligent Data Operating Layer (IDOL) Server, which collects unstructured data, can work with HP ArcSight to help security professionals identify threats from even the most advanced adversaries.

This approach to security analytics will be a central aspect of enterprise security going forward. Important clues about upcoming or ongoing attacks can be hidden among all of the data generated by the myriad systems and devices that exist in today's enterprises. An approach that can quickly find these clues and enable the enterprise to act is vital.

Conclusion

HP is developing the products and capabilities that help enterprises move beyond the perimeter approach to security by providing the intelligence and products that can disrupt the ecosystem established by attackers.

Businesses can take advantage of products and services like HP Reputation Security Monitor and HP Security Research, when used in conjunction with HP TippingPoint for network security; HP Fortify for application security; and HP ArcSight for information security, to create a holistic approach to IT security. By extending beyond the perimeter approach, a mature security program can:

- Detect threats early
- Prioritize investments and remediation efforts
- Factor in a customer's own unique threat experiences
- Prevent exfiltration of intellectual property
- Monitor and protect the reputation of the customer's enterprise

It's time to stop the cat-and-mouse game that ruled IT security for far too long and adopt a better approach.

For more information on the HP Security Research, go to www.hp.com/go/hpsr. ■

> *"Harnessing the power of analytics is nothing new for today's enterprise IT organizations."*