Deloitte.

Responding to cyber threats

A change in paradigm

Introduction

The word 'breach' has been used more in an information technology context in the last 2 years more than it had ever been in the previous 20 year before that. It is estimated that 1 billion records were compromised in 2014 (Gelmato, 2015) and at the cost of per compromise estimated to be between 52 to 87 US dollars (Verizon, 2015), the impact of these bridges to the global economy is alarmingly large. Further, a Verizon report highlighted that "organised crime became the most frequently seen threat actor for Web App Attacks", raising the concern that cybercriminal attacks are becoming more organised and systemic.

In a hyperconnected world, the ability to adequately protect data and information has been touted as an important component of risk management for a very long time by renowned security advocates like Bruce Schneier. However, with the instances continuing to rise, it seems that matters have taken a turn for the worse since Schneier first voiced his concerns some thirty years ago. The challenge has been exacerbated by the realization of Moores' law, the size of the opportunities that exist, and the Goliath's state of our security infrastructure.

The ability to combat cyber risk effectively is especially important for a country like Singapore, as it is one of the most networked and electronically connected societies in the world. Singapore's success singles it out to experience an increased level of threats as it progress towards its ambitions of being a SMART Nation. This thrust necessitates an even greater focus on the protection of digital assets. Organisations, both private and public, have a responsibility to ensure that they protect the value of their digital assets - including data, information, applications, and networks that exist within and beyond their premises, including the information that extends out through suppliers, vendors and other partners, and resides in employees' mobile devices
The traditional approach of focusing on feature, function and time to market products, systems and software increasingly incorporates security controls as a core design principle. The need to look at the data, correlate it and automate responses through the use of machine learning and a radical redesign of the foundation of our systems is key. Managing cyber risks and opportunities starts with recognising and understanding the importance of digital assets. While financial risk is important, cyber risk poses a real threat to performance and survival because most major organisations are now technology-driven, and therefore vulnerable.

In this changing landscape, a shift must take place to adequately combat the challenge. The old approach has failed many organizations and cost the world billions of dollars. While we expect that advancements in technology will continue to disrupt the way we approach cyber risk, the objectives and principles identified in this paper attempt to provide the basis of the mitigation model that is still evolving – and must continue to do so.

These mitigations are explored in the proposed Deloitte Cyber Security 3.0 model.

The new reality

Cyber of global concerns

Recently, the President of the United States, Mr. Barack Obama, signaled online security are a priority for his administration in 2015, labelling it an "urgent and growing danger" for Americans (Martin, 2015). He went further to cite the Sony hacking incident which revealed details of 50,000 employees as evidence of the link between personal data protection and the need for new cyber security laws (2015). At the same time Mr. Tony Abbott, the Prime Minister of Australia, was quoted as having conceded the Australian review of the 2009 strategy is "long overdue" and necessary for the nation to stay "a step ahead of our antagonists."

There are many studies on the future and world mega-trends to 2020. These mega-trends include SMART technologies which interact more seamlessly with human lives, SMART Cities and infrastructure, energy changes, e-Mobility, new business models, and fundamental demographic changes brought about by societal changes and advances in health and wellness and the increasing ageing population.

While technology has been a key enabler to better and more productive living, it does bring its fair share of challenges as increasingly sophisticated cyber threats become a key concern in this connected world. A recent report released by Fire-Eye suggested that hackers, most likely from China, have been spying on government and business targets in the region for over a decade (Hamzah, 2015). Such threats which are less known in the past have made way in headlines in recent years and months, a stark reminder of the cyber threats in this global connected community. Zaid Hamzah, a cyber-security legal strategist, quoted Gartner predicting that more than 25% of global firms will adopt big data analytics for at least one security and fraud detection case, up from 8% currently. The issue is best summarised by the quote that "Every CIO and CISO wakes up each day knowing that if they don't get security right and breaches are suffered, their program can be perceived to be ineffective, and their citizens may suffer direct harm." (Decker, 2012)

Cyber in Singapore

As Singapore celebrates 50 years of independence in 2015, it positions itself as a SMART city and a SMART nation within the context of its standing as a global citizen.

In 2014, Mr. Lee Hsien Loong, the Prime Minister of Singapore, pointed to cyber security as an important aspect of Singapore's SMART Nation ambition. He said "We are putting more and more functions and data into our computers, handphones, network and systems. Often they know more about us than we remember about ourselves. It is vital that we have secure systems that we can trust, not just preventing credit card numbers from being stolen, but protecting ourselves from malicious attacks where there is hacking or Distributed Denial of Service attacks, you know what that is. Whether is it malware that infects our computers which steals sensitive information or possibly threatens critical infrastructure if it gets into the hospital IT systems, patients can die, if it gets into our power system, our power grid can be brought down, if it gets into our airport system, we can have a very serious problem." Such concerns are voiced elsewhere by world leaders and this is becoming a pandemic which needs to be addressed seriously.

In the face of some of the hacking and cyber incidents in the recent past, the Singapore government launched the Cyber Security Agency (CSA) to better coordinate national efforts against cyber-threats and to bring about a "whole of government" approach towards cybersecurity strategy, outreach and industry developments (Hamzah, 2015). The agency chief reports directly to the Prime Minister's office to mark its importance. In addition, the strategically launched Interpol Global Complex for Innovation (IGCI) in Singapore to fight international cyber-crime marked a major milestone by both Singapore and the global community to combat cyber-threats. These examples show the government's ongoing responses to boost efforts in tackling the new and emerging crimes in Asia Pacific and around the world.

Cyber trends and the future model

Megatrends of cyber security

Since 2010 the world has seen a significant increase in cyber-attacks across the globe, as the level of sophistication of cybercriminals has progressed in tandem with that of Moore's law and the threats that they pose to targeting organizations is no longer random in nature. To effectively tackle these issues requires an understanding of the actors, their level of sophistication and their determination:

Despite efforts from organizations these attacks show no sign of slowing down. The level of sophistication and the capabilities of the perpetrators continue to grow: data has shown that the combined power of an insider threat allied to organized crime is most dangerous.

Figure 1 is a graphical illustration of Threat Actors and Attacker Determination. The participants use a variety of techniques to achieve their end objectives as shown in Figure 2 which summarises the techniques and the vulnerabilities that the threat actors focus on. The root cause from studying the corporate challenges is the attitude that we adopt in addressing the issue. Each of the challenges is usually addressed individually instead of abstracting them to uncover that there is a fundamental flaw. The silo approach to "fix it" has also caused a deterioration in the way incidents are being managed thus, to use the common idiom, meaning that often we miss the forest for the trees.

Figure 1. Threat Actors

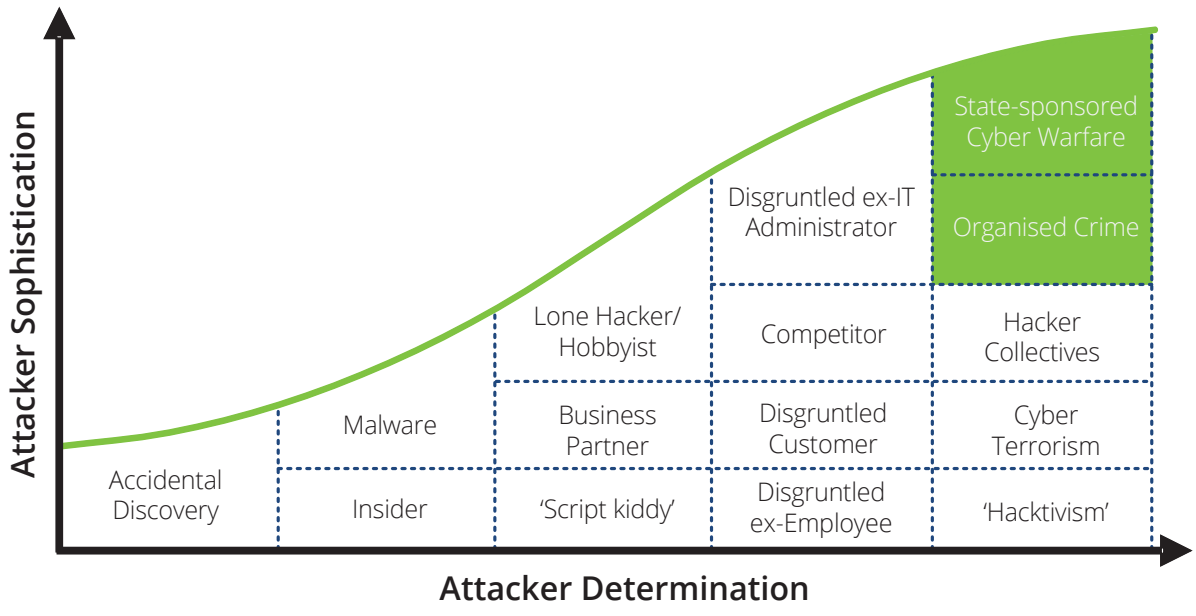
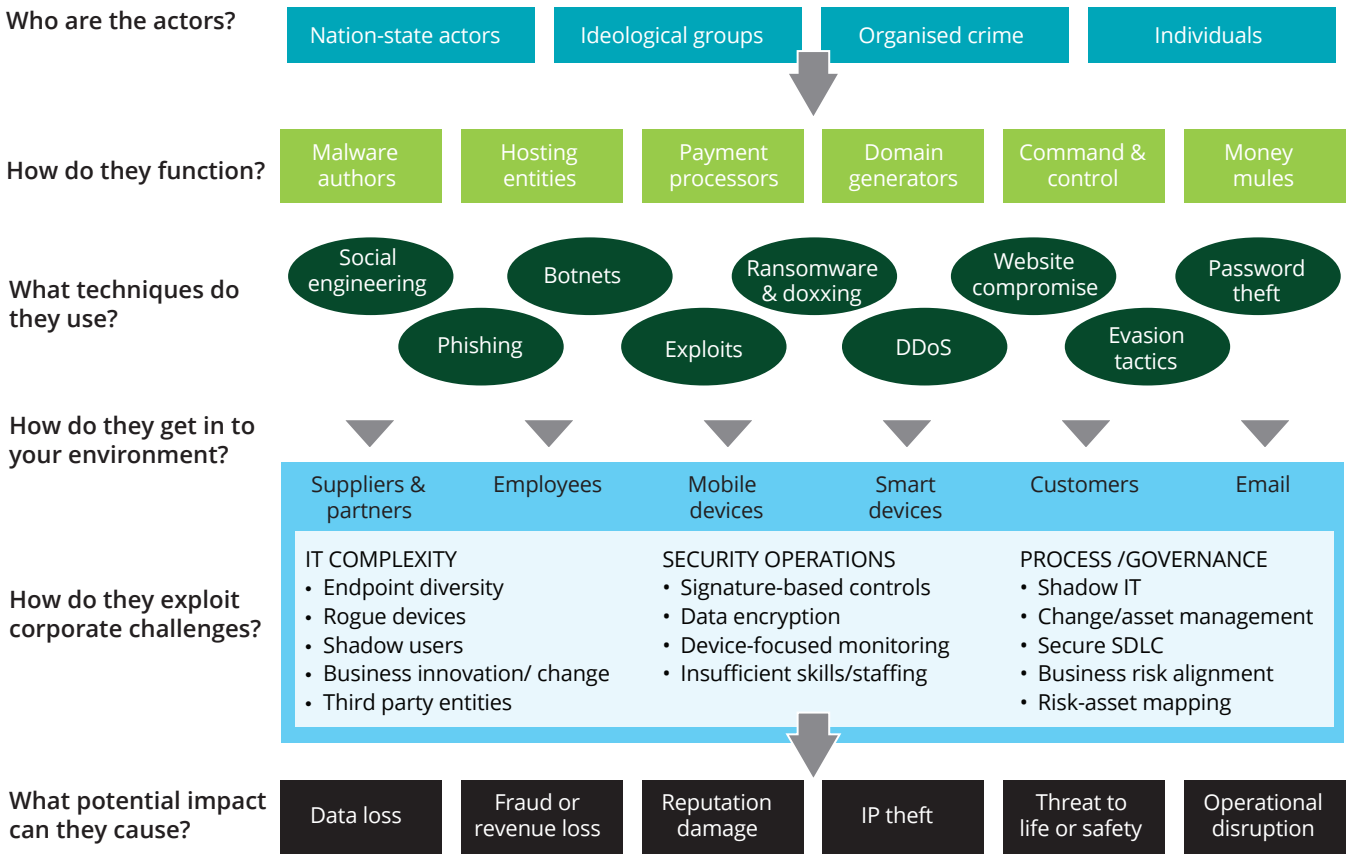
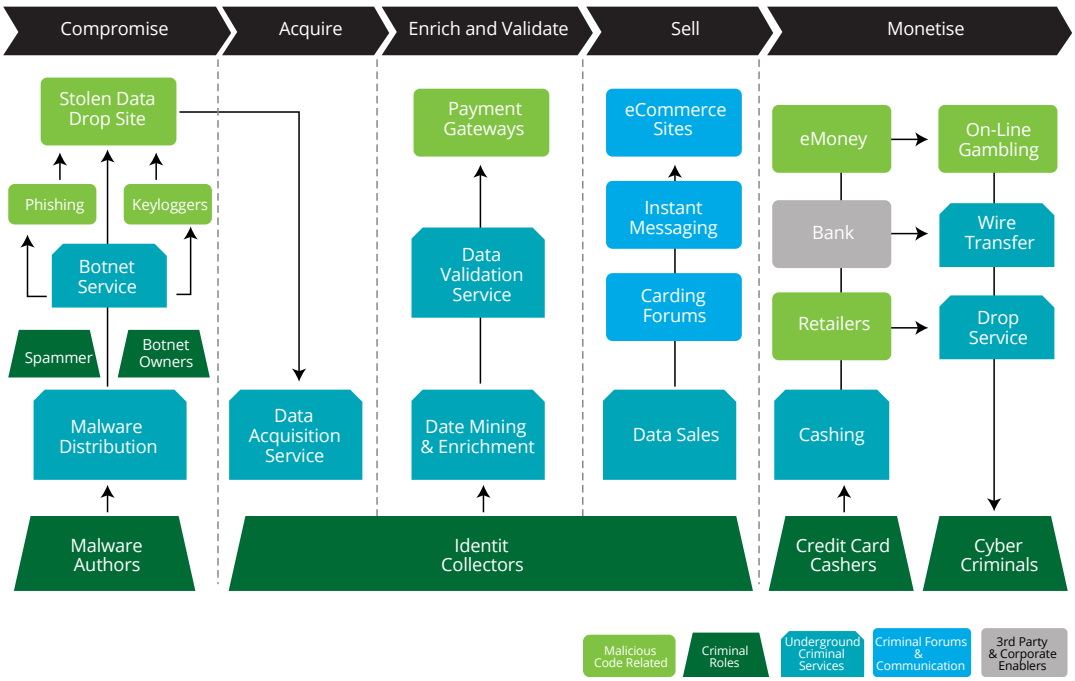


Figure 2. Summary of techniques and vulnerabilities focused by threat actions



We must understand that hackers are only one element of the cyber enterprise. Just like commerce, the underground commerce market is very similar to a typical C2B or B2B marketplace – examples from the past include CarderPlanet and Darkmarket. The monetisation of information is best depicted in Figure 3.

Figure 3. Monetization of information



In response to these relentless threats the industry has come to the realisation that they need to change the way they prepare, defend against and recover from cyber-attacks. Listed below are some of the failures and challenges faced by the stakeholders in the ecosystem.

Failure to include security and control as part of the design principles

Traditionally, IT infrastructure has been focused on providing functionality and efficiency. The application, the network and the server infrastructure have been driven by business strategy, operational requirements and of late, meeting M&A requirements. Constantly increasing business demands has led to the implementation of security and the relevant controls as an afterthought.

Even with contemporary system development methodology such as Agile, the state of security has not improved. This largely has been the ethos of the IT industry as security and controls have often been an afterthought, and this was even part of the design principles of the underlying architecture. Courtot suggested that the suboptimal performance of security and controls in countering threats owes its heritage from a "bolt" on mindset (Courtot, 2015). These principles and approaches have been used as the foundation of the technology used by organisations since computerisation took place, but they have been ineffective. It is time for a revamp.

Addressing the incident and failing to detect campaigns

Very often, first responders of incidents attempt to clean up and push to eradicate the issues on hand. Incident response is often a marathon rather than a sprint but most respondents to an incident are too anxious to "clean up" and fail to conduct a root cause analysis.

The phases of a typical attack illustrate the fact that most perpetrators today have a long view and focus on monetisation. To return to our idiom, focusing on the trees is an approach that has long been demonstrated by IT professionals owing to the lack of resources but also the desire to demonstrate results. This sometimes becomes counterproductive as it means that eradication is not effective. A report by the Ponemon Institute in 2013 best described this issue by highlighting that advanced attacks usually goes undetected for an average of 225 days. But, as the old Chinese saying states – 斩草不除根,春风吹又生 – which translates as 'when cutting down weeds, first you must get rid of the roots, otherwise, the weeds will return in Spring.'

Implications arising from the shortage of competent cybersecurity professionals

The widespread shortage of cybersecurity professionals is posing a significant challenge for organisations. In a report published by Rand Corporation (Libicki, Senty, & Pollack, 2014), it was identified that this issue poses the most significant risk to the US Federal government. This phenomenon is not limited to North America but is worldwide in nature.

In response to the need to shore up their cyber security capabilities, many organisations look to outsourcing to services providers – and not necessarily even to organisations that focus on cybersecurity. These include service organisations that have traditionally focused on providing infrastructure, network and application development.

However, owing to the shortage and the strong demand, many have now started to provide security services – engaging these opportunistic service providers may not be the most appropriate strategy for handling cyber security.

Ineffective threat analytics

Security information and event management ("SIEM") solutions have existed for an extended period of time. Their effectiveness in providing a view of the security posture and to provide pre-emptive warning of compromises has been questioned owing to:

- Failure to provide insights from traditional anomaly analytics;
- Misconfigurations owing to complexity;
- Inability to operationalise such analytics;
- Lack of skilled resources to interpret and infer the analysis; and
- Lack of standardised measures or models.

This view is echoed by Rochford (2014), in his report identifying the pitfalls of SIEM, where the issue of failure lies in the monitoring of noise; the lack of sufficient context; and the lack of resources.

These issues coupled with common other mistakes – failure to plan, failure to define scope and being overly optimistic in scoping – were the pitfalls of SIEM implementations. This has not stopped CIOs and CISOs aggressively positioning SIEM as a silver bullet, to the extent of engaging 3rd party service providers to assist in monitoring.

The promise of SIEM was that it will provide a view that in turn will help CISO in their identification of trends and patterns. This has generally not been fulfilled, and more often than not has led to the conclusion that security analytics carries high transaction costs and fails to yield the results it was intended to achieve. Ultimately, such failure has also led to the lack thereof of actionable intelligence, resulting in exfiltration of data and information by both internal and external perpetrators.

Cyber threats – then and now.

Imagine that you built a wall to protect something valuable. Now imagine that someone breached these defenses by flying a drone over the wall. Building the wall higher will not protect you in this new reality. You now need to fundamentally revisit your notion of what security is: the wall no longer suffices.

Therefore, in this new era of cyber threat, governments and organisations around the world are realizing that a paradigm shift is necessary to counter the emerging megatrends that are rendering the old defenses ineffective. A new model is warranted and that leads to the development of the proposed Deloitte Cyber Security 3.0 model.

Deloitte Cyber Security 3.0 model

Throughout the past decade, most organisations' cyber security programs have focused on strengthening prevention capability based on established information assurance strategy: defense-in-depth. This approach advocates a multi-layered approach to deploying security controls with the intent of providing redundancy in the event a security control fails or a vulnerability is successfully exploited in one of the layers.

The belief that this is sufficient creates a misguided perception that adversaries will be successfully thwarted by the multi-layers of defense in place. The rise of APT attacks and the Stuxnet success clearly demonstrated the fallibility and danger of such a false sense of security: the myth that compromise has not taken place is widespread.

Once an organisation accepts that they will eventually be compromised, they must incorporate and enhance their level of detection and response capability in addition to securing it further through the adaptation of new design objectives and principles for applications and networks. In this way, when the actual compromise happens, an organisation is well-positioned, prepared and ready to respond immediately and effectively to the threat and stop the 'bleeding'. It should be realised that prevention and the defense-in-depth strategy remains relevant and necessary in cyber security programs, but that in itself is no longer adequate and must be complemented by a resilient detection and response capability. The objectives of the Deloitte Cyber Security 3.0 model are principled on being: secure, vigilant and resilient.

Secure: Enabling enterprise business innovation by protecting critical assets against known and emerging threats across the cyber ecosystem, as well as establishing a mature detection and response capability. Being secure means understanding and focusing protection around the most risk-sensitive and valuable assets, and establishing risk-prioritised controls in compliance with industry standards and regulations.

Vigilant: Reducing detection time and developing the capability to continuously monitor and effectively respond to cyber threats. Organisations must establish situational risk and threat awareness across the environment to detect violations and anomalies that may indicate, or even predict, compromise of critical assets.

Resilient: Identifying critical "single points of failure" to develop alternative back-up mechanisms and strengthening recovery capability when incidents occur. Organisations must establish the capability to manage critical incidents, rapidly contain the damage, quickly return to normal operations, and mobilise the diverse resources needed to minimise business disruptions, as well as impact to reputation and brand damage. Rather than being a necessary burden, the cyber risk program is a positive aspect of managing business performance.

The design principles of the model are explored in the following pages with these objectives in mind.

Design Principles: the realisation that everything is a threat and security must be incorporated in the core

There is a need to review and rethink the design principles. When the team in Mercedes designed their F1 car for the 2014 season, after a disappointing performance the year before, they took a completely different view and designed every single component to complement each other. The result yielded a championship team for both driver and constructor. Organisations must think about their cyber security in the same way.

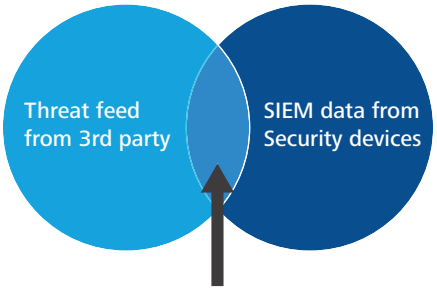
The design principles that have existed within the information technology fraternity for many years have – and will always be – primarily for the advancement of exchanges and fulfillment of business needs. However, the principles must now incorporate security as part of the core. There is a need to assume that everything and anything will be a threat to the organisation. As a result, new design principles have been suggested (Doherty & Banerjee, 2015) which attempt to address this challenge by:

(a) Isolate and segmentise;
(b) Unit level trust and least privilege; and
(c) Ubiquity and centralise control.

There is a need to consider designing the system as a whole and focusing on ensuring that each component can be secured and monitored. When incidents are detected, the resiliency objectives are then applied to ensure that they remain compartmentalised.

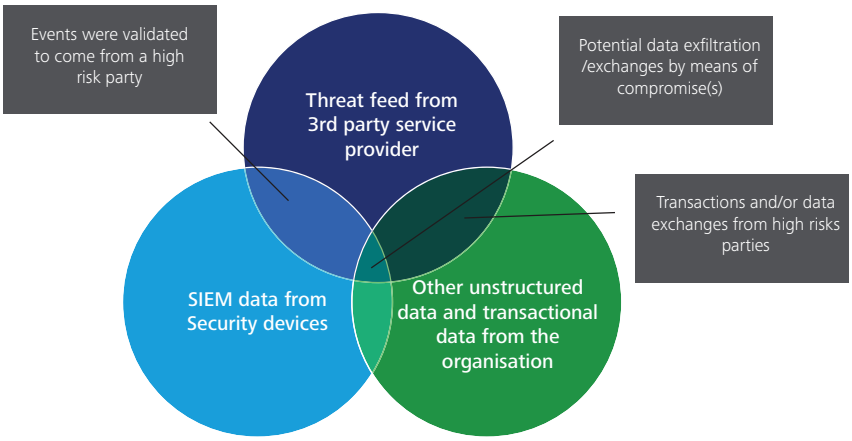
Actionable Threat intelligence is a key element of threat-centric defense.

How do you link data and events to establish relationships? Traditional methods focus only on the internal data and the use of rules to correlate and attempt to identify the perpetrator. This approach that predominantly been used for compliance reporting and alert notifications has become ineffective. The analysis of events via eyeballing patterns, flagged by a rule base engine that was configured using trial and error, is effectively a needle-in-a-haystack approach.



The union of these 2 data sets provides a high level of confidence of potential compromises within an organisation but it must be further validated

The use of threat feeds to support an organisation in the identification, detection and prevention of cyber-attacks is now seen as the more effective method and reduces the errors associated with human identification processes. Essentially, the methodology correlates events that are being collected within an organisation with threat feeds in real time to provide "intelligence". This approach supports the threat-centric monitoring and detection process by delivering feeds of threat-related indicators, commonly known as indicators of compromise (IoC). Through the analysis of detected threats against these indicators, organisations can proactively deploy relevant correlation rules, detection indicators and signatures for the identified threat-related activity in an attempt to eliminate the threat before it reaches the targeted asset.



The analysis of data with external threat feeds creates actionable intelligence for the monitoring team and facilitates the response process of an organisation. It also expedites the investigation of security incidents by providing the information and context on the adversary's tactics, techniques, and procedures. Further, by incorporating risk assessments, organisations will be able to improve their prioritisation of implementing security controls.

However, could this be further enhanced? The layering of additional structured and unstructured enterprise data provides greater level accuracy and predictive insights into the state of the organisation's security affairs. Further, the use of an intelligence platform to consolidate and refine information to actionable intelligence becomes important as the correlation of the information facilitates the use of limited resources to effective counter potential cyber insurgence.

Revamp the Intel and Information sharing among security practitioners

Crowdsourcing is a concept many are familiar with to raise funds and ideas. The concept has also been widely adopted in the cyber arena. From the hacktivist group Anonymous to the cybercriminal group Carder, the concept of Crowd has been well utilized. They share, exchange and trade intelligence and techniques among themselves to enhance their level of success.

In the US, the initial idea of sharing was mooted in 1999 to address the increased risk perceived by cyber criminals. The establishment of the National Cybersecurity & Communications Integration Center by the Department of Homeland Security was the realisation of this concept. The centre is intended to provide "24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement" (Department of Homeland Security, 2015).

The concept of private information Sharing and Analysis Centers (ISACs) has been deemed as a valuable source of information for information security managers (Granneman, 2013), but it has not been widely adopted and the concept is seldom used among security practitioners. The reality is that sharing creates the opportunity to stop compromises, as demonstrated in the number of cases where near misses have been stopped and the increase in ability to apprehend high profile perpetrators.

However, often organisations are reluctant to share information and intelligence, citing restrictions placed on them by regulators and hiding behind the veil of "confidentiality" to restrict sharing – citing the fear that sharing will result in "letting the outsider" know too much. An opportunity exists for the establishment of a trusted exchange, where organisations and their external service providers (both product and services vendors) could register, exchange, validate and thereby enhance the state of actionable intelligence.

Automation as a means to address the scarcity of skilled resources

The issue of scarcity of skilled resources is a problem that cannot be solved overnight. The risk associated with the shortfall "may leave the United States ill-prepared to carry out conflict in cyberspace" (Libicki , Senty, & Pollack, 2014) and they are not the only one. The call for automation is quite clear.

However, as Geer observed: "One can only conclude that replacing some part of the human cybersecurity worker's job description with automation is necessary (Geer, 2012). If the threat space is expanding by X to the Y, then the defense has to arm up accordingly. An accelerating share of the total cybersecurity responsibility will have to be automated, will have to be turned over to machines." Thus, the need to exploit automation will likely to enhance quality and capability of the team.

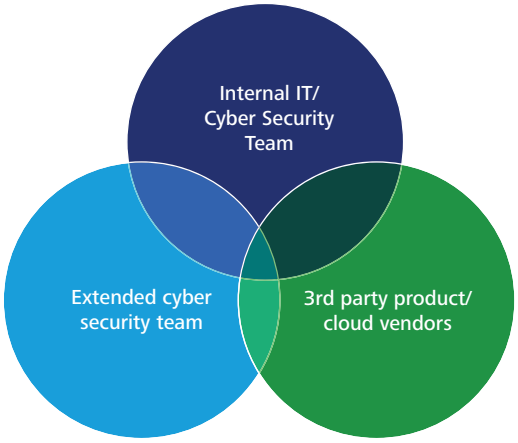
Observations made in the 2015 Verizon report showed 90% of the errors of security decisions were inappropriate because they were made by humans (Verizon, 2015). The inference of this has to be the fact that automation has not been successfully exploited. Many are confusing hard work with results, and in managing security it is the latter that will keep commerce going.

The scarcity of competent resources means that automation is a need that must be fulfilled. The lack thereof to date has been attributed to the lack of confidence within the community even though technology allows for such automation – a lack of confidence that may be overcome with accurate actionable intelligence as described previously. With the deployment of actionable intelligence, the opportunity exists for the team to automate operational security to reduce the margin of errors compared to if they were performed by humans. An example of such an operational security event may include the management of an incident at the end point where the nature of the event is routine and the investigation, mitigation and remediation processes could be automated together with user education and certifications. The opportunity to automate is quite large, but there is a need to manage risk to ensure that the defender does not stop and become invalid in identifying and addressing challenges.

The power of combating crime together

When combating cybercrime there is a need to act together: coordinating between the internal and external security provider.

The concept of "I can manage and handle all" is not possible in a resource scare situation, and many organisations lack the required resources to be self-sufficient. Very often, an extended team is used to perform operational and attestation tasks but very seldom they are integrated into the overall cybersecurity framework to enhance the overall secure and response capabilities of the organisation. This is often the observation both in the commercial and public sectors around the Asia Pacific region. The treatment is the same for most third party product vendors. The lack of integration creates unnecessary blind spots that are taken advantage of by cyber criminals that are sharing and integrating and coordinating their attempts to compromise an organisation.



There is a need to rethink our outdated notions of how threat actors research and behave and then apply this to plan how security practitioners should operate: integrating and coordinating among all three parties to secure, update and remediate an organisation's prized assets.

In summary, the proposed Deloitte Cyber Security 3.0 model has 3 objectives - secure, vigilant and resilient - woven together with 5 design principles of:

a) Incorporating security in the core design
b) Applying threat intelligence in the core design
c) Sharing of intel and information among security practitioners
d) Automating processes to address the scarcity of skilled resources
e) Enabling the power of combating crime together

Conclusion

As Andrew (2014) suggested in his book, technology is at an inflexion point, where significant progress in areas like healthcare and transportation will be transforming the way society progresses. However, we must ensure that the security risk associated with such transformations is adequately managed through a harmonised methodology integrating people, process, technology and most importantly data into the management and decision-making process.

The many recent high profile cyber breach cases have reinforced the notion that no organisation is immune to being targeted and compromised, despite the best cyber security defenses deployed. Clearly there is a need to recognise the need to shift our perceptions on cyber threats of the future and reconsider our approach to anticipate, respond and manage them from a more holistic perspective.

As connected countries like Singapore move towards the SMART nation initiative, aided by the increase in Internet of Things (IoT), "..cyber security is a key imperative that businesses need to think about in safeguarding their operations" and it is recognised as a "national security imperative that we need to recognise and be adequately prepared for" (Iswaran, 2014).

We must challenge the assumptions, the methods and the mindsets of the past if cyber security practitioners are to be effective. A new paradigm is required where practitioners partner the management and the boards of organisations to take bold steps to respond to – and anticipate – the evolving landscape. The application of traditional methods and technology is no longer as effective, and thus the call is for the industry to achieve the 3 objectives of security, vigilance, and resilience in the design of their cyber security programmes. By applying a unified approach of integrating, sharing and automating, it is possible for the global community to effectively manage the risk of the cyber threat and stay one step ahead of the cyber criminals.

This proposed Deloitte Cyber Security 3.0 model aims to address the concerns highlighted in the trends and the new normal. As the landscape evolves, so too will the model, to keep pace with the changes. This journey is continuous.

Bibliography

Courtot, P. (2015, April). Cloud without borders. RSA Conference 2015. San Francisco, CA, USA: RSA.

Decker, B. (2012). Deloitte-NASCIO Cybersecurity Study: State government at risk: a call for collaboration and compliance. Deloitte.

Department of Homeland Security. (2015, April 27). About the National Cybersecurity and Communications Integration Center. Retrieved from Department of Homeland Security: http://www.dhs.gov/about-national-cybersecurity-communications-integration-center

Doherty, S., & Banerjee, D. (2015). Orchestrating Software Defined Networks (SDN) to Disrupt the APT Kill Chain. RSA. San Fransico: RSA.

Forrester Research . (2013). Five Steps To Build An Effective Threat Intelligence Capability. Forrester Research.

Geer, D. (2012). People in the Loop: Are They a Failsafe or a Liability?

Gelmato. (2015). Breach Level Index. Gelmato.

Granneman, J. (2013, May). Information Sharing and Analysis Centers: Getting started with ISACs. Retrieved from Tech Target: http://searchsecurity.techtarget.com/answer/Information-Sharing-and-Analysis-Centers-Getting-started-with-ISACs

Hamzah, Z. (2015). Predictive prevention needed to neutralise cyberthreats. Singapore: Today.

HP. (2015). Cyber Risk Report 2015. HP.

IBM. (2013). X-Force Mid-Year Trend and Risk Report. IBM.

Iswaran, S. (2014, October 01). 2014 National Security Conference at Suntec Singapore Convention & Exhibition Centre - Opening Address by Mr S Iswaran, Minister, Prime Minister's office, Second Minister for Home Affairs and Trade & Industry. Retrieved from Ministry of Home Affairs: http://www.mha.gov.sg/Newsroom/speeches/Pages/2014-National-Security-Conference-at-Suntec-Singapore-Convention---Exhibition-Centre---Opening-Address-by-Mr-S-Iswaran,-Min.aspx

Lee, A. (2015). Cybercrooks using social media to gain people's trust. Singapore: Today.

Lee, H. (2014). Transcript of PM Lee's speech at Smart Nation Launch.

Libicki , M. C., Senty, D., & Pollack, J. (2014). Hackers wanted : an examination of the cybersecurity labor market. Santa Monica, CA: Rand Corporation.

Martin, S. (2015). Hackers expose cyber flaws. The Australian, 1.

McAfee, A. (2014). The Second Machine Age. W.W. Norton.

Ponemon Institute. (2013). The State of Advanced Persistent Threats. Ponemon Institute.

Rochford, O. (2014). Overcoming Common Causes for SIEM Deployment Failures. Gartner.

Verizon. (2015). Data Breach Investigations Report. Verizon.

Contacts

SEA and Singapore

Thio Tse Gan
Executive Director
+65 6216 3158
tgthio@deloitte.com

Eric Lee
Executive Director
+65 6800 2100
ewklee@deloitte.com

Siah Weng Yew
Executive Director
+65 6216 3112
wysiah@deloitte.com

Edna Yap
Director
+65 6531 5016
edyap@deloitte.com

Leslie Moller Director
+65 6800 2333
lesmoller@deloitte.com

Indonesia

Sigit Kwa
Associate Director
+65 6800 2903
skwa@deloitte.com

Malaysia

Megat Mohammad Faisal
Executive Director
+60 3 7610 8863
mkhirjohari@deloitte.com

Ho Siew Kei
Senior Manager
+603 7610 8040
sieho@deloitte.com

Philippines

Maria Carmela Migrino
Director
+63 2 581 9000
cmigrino@deloitte.com

Thailand

Parichart Jiravachara
Executive Director
+66 2676 5700 ext. 11913
pjiravachara@deloitte.com

Pinyo Treepetcharaporn
Director
+66 2676 5700 ext. 11946
ptreepetcharaporn@deloitte.com