WYNYARD GROUP
HIGH CONSEQUENCE CYBER CRIME:
THE CRIME OF THE CENTURY

WYNYARD™

NEW APPROACHES TO THE CYBER RISK THAT DEFINES OUR GENERATION.

Organised criminals are using new tactics to put a new face on old crimes, and with overwhelming success: Headlines of financial loss and reputational damage are common place as organisation after organisation report a cyber breach. Research suggests that on an average it takes 256 days from the initial compromise of a network until a company realises that it has suffered a loss. Better analysis of network data is emerging as a powerful defence helping Australian companies to harness the power of analytics to detect breaches early and minimize their exposure.

As long as humans have formed societies, marginal elements of those societies have engaged in all manner of crimes. Theft, fraud, extortion and other asset-related offences have persisted for millennia, and continue to be fundamental elements of everyday human activity. Crime is an unsolvable problem that is, at best, managed, remediated and punished based on the extensive investigations of law-enforcement authorities.

The advent of computers, and of networks linking them, has seen long-extant crimes brought into the modern age – becoming increasingly devastating as society has become more broadly and deeply interconnected. Driven by the promise of financial rewards and empowered by the sheer scale and reach of Internet-based attacks, organised criminals have secured an increasingly strong foothold online as they refine their skills in large-scale, high-consequence cyber-crime (H3C) – deliberate criminal activity that has a “severe” or “critical” operation, reputational or financial impact.

The recent hack of UK telco TalkTalk shows the magnitude of the problem: two 15-year-old and 16-year-old boys were recently arrested for stealing 21,000 unique bank account numbers, 28,000 obscured credit and debit card details, 15,000 dates of birth and 1.2 million customer email addresses, names, and phone numbers. Unconfirmed reports suggest that TalkTalk may be facing a $75,000,000 associated loss. Another recent breach, at the United States Office of Personnel Management, saw 21 million personal credentials stolen.

Each of these pieces of personally identifiable information has a market value for cybercriminals, who regularly on sell financial and personal details by the thousands in secretive online marketplaces. This information not only facilitates identity theft, but helps criminal syndicates improve the efficacy of criminal activity like extortion.

Adding fuel to the fire, large-scale theft of corporate data is creating new risks and operational exposure for companies obligated to protect customer information; ransomware such as Cryptolocker holds victims’ systems hostage even as other malware exfiltrates sensitive data by the gigabyte; and social-engineering strategies are facilitating the creation of massive, global botnets that are being rented to criminals on a ‘cybercrime-as-a-service’ basis.

These and other elements all play a role in an increasingly sophisticated ecosystem of cybercrime that often resembles the operations of large, legitimate corporations. Cybercriminal operations are actively recruiting CIOs, data analytics specialists, data-centre designers, security and other experts to build profit-minded underground operations. Many have their own R&D operations and others are even backed by nation-state interests that in recent years have escalated the threat of H3C to a completely new level.

“There are two types of organisations in the world – those that know they have been hacked and those that don’t know they have been hacked.”

— **Andy France**, former Deputy Director of GCHQ

OPERATING IN THE NEW NORMAL

Whether they are targeting your information or your money, the characteristics of this new cybercriminal ecosystem add up to one undeniable truth: no matter what size or industry your company might be, the threat of cyber-attacks is no longer simply theoretical – and perpetrators of H3C are no longer just fumbling around online in the hopes of finding something valuable.

Targeted attacks are aimed at compromising specific organisations and are tailored to the unique characteristics of those organisations and their employees. Breach after breach – not only of major overseas brands, but Australian icons such as Kmart and David Jones, which recently lost thousands of customers’ personal details in cyber-attacks – serve as reminders that cybercriminals are already pounding on your door.

Even worse, they may already be inside.

Statistics from the Australian Cyber Security Centre (ACSC) 2015 Threat Report highlight the magnitude of the threat to local companies. This Government-run Centre of Excellence, which unifies cybersecurity resources from six different police, defence, and specialist security bodies, reported that authorities responded to 11,073 cyber security incidents involving Australian businesses during 2014 alone. This included 8100 incidents involving compromised web sites and 1131 incidents involving government networks.

These incidents are increasingly exposing Australian organisations as the country’s history of innovation, strong resources and other industries made it a “target-rich environment for cyber adversaries”, the report warns, leading to “a range of cyber adversaries motivated to target Australian networks”.

ACSC is already recording “daily” cyber espionage activity targeted at Australian government networks and a rising tide of attacks on corporate networks, where breaches can significantly affect company reputations, profitability, and ability to compete in the global economy.

Industries including energy (29 percent of attacks), banking and financial services (20 percent), communications (12 percent), defence (10 percent), and transport (10 percent) were the most frequently-targeted, with 153 of the reported incidents involving “systems of national interest”, critical infrastructure and government.

“This type of activity is no longer opportunistic,” the report’s authors concluded. “It is now an activity targeting Australian government and businesses.”

In the new normal, there is a recognition that cybersecurity breaches are inevitable; their perimeters broken by changes in technology and usage models, business and information-security executives face a perfect storm of threats as they work to change their strategic position regarding cybersecurity.

The world is well past the point of pretending that breaches can be stopped cold, the conventional wisdom now says; the default position must now be an acceptance that breaches are going to happen. While layered or ‘defence in depth’ models are still important, an effective cybersecurity defence must now be focused on rapid detection of malicious activity rather than its prevention.

Empowered by executives and boards that are rapidly realising the risk that H3C poses, CISOs must arm their teams with tools to identify anomalous security activity and gain an unprecedented view of its true cybersecurity exposure. This exposure, in turn, will not only help monitor for cybercriminal activity but will help prioritise the investment of further time, money and effort around IT security.

Reducing an organisation’s cybersecurity exposure will reduce the chance that cybersecurity compromises may adversely impact a target organisation. This directly translates into improved assurance by executives and corporate boards, providing increased confidence on the part of corporate risk officers (CROs) and others whose job it is to ensure the business addresses cybersecurity within its overall handling of operational risk.

SHAPING AN ORGANISATIONAL RESPONSE TO H3C

Recognition of the new cybercrime threat has elevated cybersecurity concerns to the top of business executives’ priority lists. A recent survey of 112 CIOs by US investment firm Piper Jaffray, for example, found that 75 percent expected to increase their spending on security in 2015 – an increase from 59 percent last year. Gartner’s latest projections puts growth in information-security spending by Australian companies at 7.4 percent annually, well ahead of the worldwide growth average of 4.7 percent.

The Telstra Cyber Security Report 2014 tied this growth to the growing profile of information security as a C-level concern: 84 percent of companies in that survey said that CEOs, CFOs and COOs were involved in the final stages of deciding on IT security spending, with CTOs and CIOs involved in a further 74 percent of those decisions.

Interestingly, recent **Ponemon Institute research** found that while the average cost of data loss had jumped to $US154 per record in 2015, involvement of board members in cybersecurity strategies reduced this by $US5.50 per record.

Security has, in other words, evolved from being a purely IT-related concern, to becoming a strategic business function that is most appropriately handled at the highest level. This important change mirrors the growing professionalism of cybersecurity attackers, who have evolved from the stereotypical basement hackers into consummate professionals that are increasingly developing well-funded, well-resourced professional networks that incorporate some of the world’s best IT talent.

Cybercrime offers many appealing characteristics for criminals, since it allows them to act at a much larger scale, and at a distance from their targets. This significantly reduces the chances they will be caught and may also deliver massive windfalls that are hard for cross-jurisdictional law-enforcement efforts to identify and act upon.

Indeed, investigations suggest that many of today’s largest cybercriminal operations are linked to longstanding criminal syndicates that have used the Internet to put a new, modern face on age-old crimes like extortion, money laundering, and fraud.

Many cybercriminals use telltale signs to identify unpatched targets vulnerable to known weaknesses. This might be data calls structured in a format known to be specific to a certain version of a particular server software, for example, or innocuous protocol responses to generic queries.

Cybercriminals readily share this information with each other, building large databases of intelligence that provide frightening insight into the technological underpinnings of modern businesses. Over time, this information is collected and harvested to identify potentially vulnerable organisations of interest – and cybercriminals hone in on their targets.

Time after time, hackers have slipped into corporate networks and spent days, weeks, or months exploring the network resources available online. Malware may quietly collect sensitive information as it traverses the network, harvest users’ Internet sessions looking for passwords, send corporate documents or databases to cybercriminals outside the party, or simply sit waiting for an external trigger to take a particular action such as deleting critical business information.

Studies suggest that it can take many months – an average of 256 days in the Ponemon Institute research – before a company identifies malicious attacks that have likely already exfiltrated masses of sensitive corporate information to their outside criminal masters.

“Data losses do not occur at the moment a breach takes place. Typically malware spends sometime surveying the network, looking for weaknesses and compromising user accounts with high access privileges,” says Jon Piercey, APAC Vice President, Wynyard Group. “It might be weeks while the criminals establish a position where they can exfiltrate valuable data.”

This ‘attack timeline’ is a double edge sword for the CEO. On the downside, breaches that have laid undiscovered for months have forced the resignations of CEOs who learned the hard way. On the upside, the timeline provides an opportunity to identify the breach before significant data loss. This is where clever analytics looking for this anomalous behavior provides the advantage.

ANALYTICS: EXPOSING THE HIDDEN CRIMINALS

Even as the desire for better risk management drives awareness of H3C and its potential effects, security-analytics technology is equipping corporate cybersecurity teams and third-party cybersecurity providers with unprecedented operational visibility.

While perimeter defences are absolutely important in providing a certain level of protection against known security attacks, analytics offers the best hope for organisations needing to identify the 'first seen attack' with no known signature, that has evaded the perimeter defences.

Indeed, any organisation that has a built-in 'defender's advantage': (knowledge about the layout and operation of the network that intruders do not normally have) is more likely to be able to defend themselves more effectively. You should, after all, know your network better than anyone else – and that puts you in a strong position when defending it.

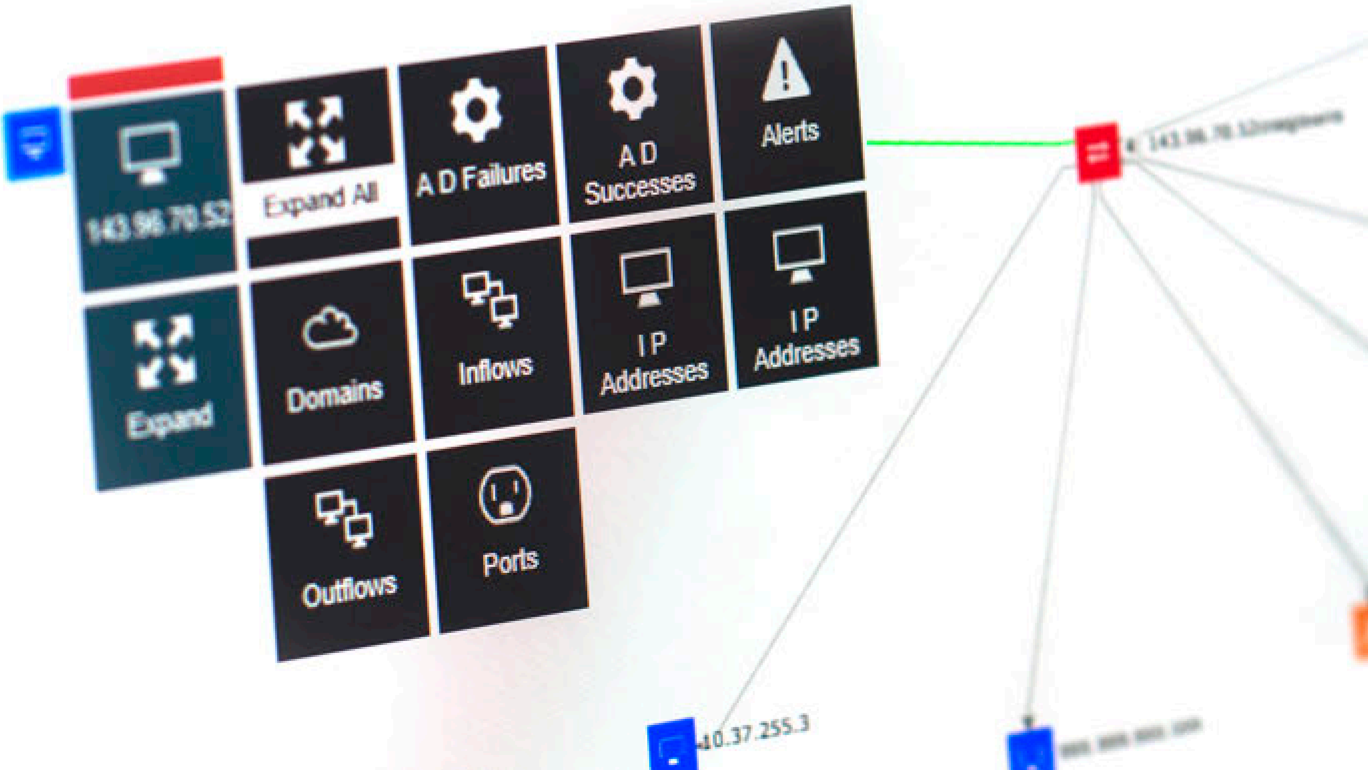
Cybercriminals, on the other hand, need a vulnerability to exploit and time to exploit it. The process of exploring a victim network leaves traces in network-activity logs, and these traces can be picked up with the right threat-analytics approach.

Many companies have struggled to derive value from the huge volumes of log data their networks generate. However, today's analytics platforms are designed to scale enough that they can extract new value even from old data that has never been made the most of.

By using analytics tools to process large volumes of security log information, organisations can baseline normal network activity, then quickly detect and act upon anomalies that suggest criminal activity is occurring. Attackers may be able to steal privileged-account credentials to gain access to your network, after all, but they aren't likely to know exactly how your users normally interact with online services and business applications – and this opens up an opportunity to catch the perpetrators of H3C in the act.

Analytics is a key component in the five 'knows of cyber security' that Telstra CISO Mike Burgess says are critical to getting – and keeping – control of your cyber security exposure. These include:

1. **Knowing the value of your data.** Some data has a much higher impact on the business than other data, and with resources typically limited it's important to know which data is the highest priority to protect. It's also crucial to remember that what an IT executive thinks is important may be completely different than what a business leader sees as important.
2. **Knowing who has access to your data.** Management of privileged accounts has emerged as a major problem as study after study confirms that users are much worse at protecting their passwords than they should be. This is why it's important to ensure that access to data is limited to those who need it – and making sure you continually monitor that list as the business changes over time.
3. **Knowing where your data is located.** Particularly in today's cloud-heavy computing environments, data may be stored on servers anywhere in the world as easily as being stored on your company servers. Tracking physical, virtual and derivative instances of your data across external service providers is therefore of paramount importance.
4. **Knowing who is protecting your data.** You may think your IT department has your data under lock and key, but relationships with service providers can change this. Make sure you are aware of any and all third-party providers involved in the storage, backup, recovery, archiving, and disposal of the data lifecycle: their security practices are just as important to your overall risk profile as your own.
5. **Knowing how well your data is protected.** If you don't know exactly what applications, technologies and devices your data is exposed to at every point in its journey, you are potentially leaving it exposed to attacks by cybercriminals who actively seek out and exploit often obscure weaknesses. Stay on top of new cybercriminal attacks and move quickly to apply patches for new vulnerabilities as they are discovered.



These guidelines apply equally to any corporate asset: knowledge is power, after all.

A key to better handling cybersecurity is to ensure that it's treated at every level with the same significance as conventional crime has been regarded for decades. "In the end, it's just a crime," said Burgess, who has been leading Telstra's IT-security efforts with a strategy built around the ideas encapsulated in the 'five knows'.

"It might be a little bit complicated, but if we think long and hard across the rest of our businesses, we have complicated risks elsewhere and we are capable as humans of dealing with those. But you do need to educate yourself."

Analytics provides that education – and with the right approach, it can deliver benefits to security-conscious organisations against a cyber compromise that could have a high consequence impact. These benefits are further enhanced with the application of best-practice security guidelines like the Australian Signals Directorate's (ASD's) Top 4 Strategies to Mitigate Targeted Cyber Intrusions, the Protective Security Policy Framework (PSPF), and the Digital Transformation Office's (DTO's) Digital Service Standard (DSS).

There is no lack of information about how to improve cybersecurity defences; the key is following that guidance, and backing that effort with the appropriate tools to facilitate an effective cybersecurity response.

These tools may be used in-house or run by third-party operators, who maintain security operations centres (SOCs) on behalf of their clients. Reports can be easily made available to clients, who can use visualisation tools to review and act upon threats much faster than they could do by themselves. This, in turn, allows IT-security professionals to accomplish more with less – and to react instantly when cybercriminal activity is detected.

"Analytics gives you the opportunity to strike back in the early days," Piercey said. "It lets you understand what unknown unknowns are happening on the network, why this behaviour is taking place, and what it's doing."

"It's a journey of discovery – and figuring out the unknown unknowns isn't just a smart thing. It's a critical thing to do for your business."

APPLYING PROVEN REAL-CRIME SMARTS TO CYBERCRIME

While the persistence and resourcefulness of today's cybercriminals has put many organisations on the back foot, better use of network information offers a chance to turn the tables by leveraging the most potent source of information that companies have.

Recognising the growing profile of cybercrime as a significant threat to any business or government organisation, Wynyard Group has built on the success of its Advanced Cyber Analytics (ACA) solution to apply its well-developed algorithms and analytics capabilities to the investigation of HC3 activities.

The result is **Advanced Crime Threat Analytics** (ACTA), a user and entity behavior analytics solution with proactive cyber forensics capabilities that applies Wynyard Group's proven analysis techniques to large volumes of network log data.

Whereas conventional security solutions use rules (to know what "normal" looks like) and signatures (to know what bad looks like), threat analytics techniques monitor network activity for previously unknown compromise – things that have never before been seen and are unknown to exist on the organisation's network. This anomalous activity can be detected within the logs of security software, network hardware devices, or user behaviour – all holding essential information that forms a powerful body of evidence that companies can leverage to fight back against unwanted intruders.

"Analytics delivers the information you need to understand what's normal in your network and what's abnormal in your network," said Piercey. "The only advantage you can have over these attackers is knowing what's happened and what has changed."

ACTA incorporates a range of capabilities that make it an invaluable tool for discovering the hidden threats on corporate networks. As opposed to many existing security solutions, it monitors activity across the entirety of the network – ensuring that anomalous behaviour is detected even on networks that have already been compromised.

Use of advanced probabilistic machine-learning techniques – developed and refined within the Wynyard Crime Science Research Institute over years of ACA use in real-world criminal investigations – puts well-developed algorithms onto the task of finding the proverbial needle in a haystack – the never before seen threat or 'unknown unknown' that often opens an HC3 case wide open.

Those unknowns are usually buried within plain sight, residing within massive quantities of log data – ACTA scales to cater to very large data sets– that are collected using existing systems but often are not formally analysed due to a lack of tools or internal security skills. The system accepts a range of data (DNS, proxy, NetFlow, Remote Network Access, Active Directory, and DHCP logs) in formats including raw logs, SIEM logs, and common event formats, and can be extended to accept non-standard formats as necessary.

Taken separately, each of these data streams might not be enough to raise suspicions on its own – but analysis at an organisational level can quickly raise flags for further investigation of anomalous activity such as communications to unknown Internet servers; usage peaks outside of business hours; or logins to accounts that have been inactive for some time.

Whatever the activity, it will leave a signature fingerprint on network logs. While you may not be able to pick that fingerprint yourself by simply looking at a mountain of log data, it will be clear to ACTA that something strange is going on – and you will know immediately that there's something going on that needs further investigation.

ACTA incorporates a range of non-intrusive techniques to reduce the noise from false positives, helping prioritise the most pressing threats and ensuring that security analysts are always aware of the issues that require most urgent follow-up and further investigation. Machine-learning techniques see the platform learning from itself over time, allowing it to become even more specific in the types of activities it detects.

Combined with a range of intuitive visualisations that illustrate relationships between network elements and pinpoint common elements that may indicate threat vectors, the visual-analytics approach offers unprecedented understanding of network compromise as it happens – and not weeks or months later.

Gaining a new understanding of 'normal' is key to addressing the abnormal – and good information is fundamental to making this happen. Since HC3 activity is an unavoidable fact of life in today's world, an organised, focused response can be the difference between a minor cyber incident and a full-blown cybercriminal emergency. In the long term, the companies that survive will be those who move to proactively improve the visibility of their network – and tap into next-generation analytics tools to turn that visibility into protective action.

SECURITY IN 2015 AND BEYOND

In its first overview of the Australian cybersecurity landscape, the Australian Cyber Security Centre (ACSC) made some predictions about the key threats that organisations of all types will face into the future:

The number of state and cyber criminals with capability will increase.

Due to the limited number of quality software developers, cybercrime-as-a-service is likely to increase, reducing the barriers for entry for cybercriminals.

The sophistication of the current cyber adversaries will increase, making detection and response more difficult.

Spear phishing will continue to be popular with adversaries, and the use of watering-hole techniques will increase.

Ransomware will continue to be prominent.

There will be an increase in the number of cyber adversaries with a destructive capability and, possibly, the number of incidents with a destructive element.

There will be an increase in electronic graffiti, such as web defacements and social media hijacking, which is designed to grab a headline.

All of these attacks pose a tremendous potential reputational and operational threats to organisations – and all can be better dealt with through the application of a suitable security-analytics engine capable of picking out the anomalous behaviour they generate.