White Paper

Predictions 2019

Looking forward to next year in cyber security

Huntsman®

Defence-Grade Cyber Security

Predictions 2019

Looking forward to next year in cyber security

As the end of 2018 approaches and the last year of the decade dawns, the challenges faced by cyber security teams are a blend of "more of the same" and "let's change the approach".

2018: Reality versus predictions

Last year, our 2018 predictions were segmented into three broad areas:

- **Political** – Privacy and breach notifications, interference between politics and social media and the shaping of opinion and the regulatory drive for increased competition.
- **Technical** – Automation and artificial intelligence (AI), growing data volumes, the internet of things and open standards.
- **Business** – Increased role for security as a service, continued interest in block chain and the defence of target once viewed as softer.

Sure enough during the year there were developments in all these areas. Certainly, the continuing rise of social media as a force in political arenas cannot have been overlooked by anyone; even the manipulation of shared movie files to drive political advantage has become evident.

An increased need for self-defending and self-healing networks and other forms of autonomous security have been demanded. Vendors in many spaces have therefore been putting the finishing touches on their advanced marketing messages (even if the maturity of their solution lags behind).

In business the increased desire for managed security services that offer a blend of technical capabilities and operational or "on-demand" expert assistance has been growing ever stronger.

However, many of these trends/predictions are medium or even longer term in their scope; so, this year's paper will aim to identify and focus on specific things that are likely to happen in the next 12 months.

Predictions for 2019

“We have seen considerable evidence of efforts to influence elections through social media and the spread of what can only be termed “misinformation””

A hacked election

We have seen considerable evidence of efforts to influence elections through social media and the spread of what can only be termed “misinformation”. The Orwellian recasting of journalism as fake news and the promotion of alternative facts as reality (doublespeak?) are becoming a familiar part of the news-cycle in many countries. Truth may be stranger than fiction, but it isn’t necessarily as popular or as widely used.

With growing challenges to the security of election/citizen databases in some countries/states and the perpetual risks of electronic and online voting machines being attacked, we consider that the next logical step; actually conducting a cyber-attack more directly on an election database or voting system, is something well in scope of the playbooks of malign actors or unfriendly national states.

The US has passed the mid-terms and has until 2020 till the next presidential contest. The Australian general election will happen by mid-2019. In the UK a general election is not scheduled but conceivably may still happen sooner than the current plans require and there is the potential for another Brexit referendum (at the time of writing). Other major nations could also see political choices being made in an environment of tainted discourse but also active cyber-attack on the systems used for voter registration or actual voting itself.

These processes are a target already as has been widely reported; 2019 we may see the next step being taken in election interference through cyber-security means.

Major disruption in the utilities sector

Cyber security in the utilities and critical national infrastructure (CNI or CI) sector are the subject of many current initiatives. Companies within these sectors provide or support so much of the fabric of our society, whether it be water, sewage, power, gas, telecommunications, broadband, critical business services like marketplace providers or payment processing or transportation. There are no sectors deemed “critical” that are not under some degree of scrutiny.

This should not come as a surprise:

- Security protection for service delivery or operational technology networks and systems is often not up to the standard desired (in reality or perception)
- The CNI (or CI) sector is a known target of attackers
- The impacts of a successful attack are serious and wide reaching

These initiatives include the C2M2 initiative that originated in the US but is gaining wider adoption in Asia Pac and the EU NIS Directive that reflects continental Europe’s unease with the security of its utilities and critical service sector.

We feel that a significant and potentially serious (even deadly) infrastructure breach is overdue and waiting in the wings. There have been small scale disruptions and attacks on low hanging fruit; but the threat of a real, sustained and prolonged outage caused by cyber criminals acting with, or without, the support of a nation state is frightening and close.

A large GDPR breach and fine

> “When it comes to €multi-million GDPR fines, no one wants to be first; but in 2019 its likely someone will be.”

Now the rush to comply with GDPR has died down; with the “go live” date receding into the past mid-2018, there is a period of relative tranquillity in the privacy arena. Notwithstanding this is the September 2018 update to PECR (Privacy and Electronic Communications Regulation) that sits alongside GDPR and concerns how marketing and business communications operate. The business processes and approaches to privacy under GDPR are still relatively new and also there is a new regulatory regime in the regulation that has yet to be truly tested, including for major data breaches.

It is not uncommon for a big privacy breach or data loss to happen from time to time; and in 2019 it seems likely that there will be a major one that will become the first to have occurred under the GDPR umbrella. Despite the protections in place no business is safe – and now there are higher expectations, a significant data loss will become especially newsworthy as well as having a time pressure on reporting it.

When it comes to €multi-million GDPR fines, no one wants to be first; but in 2019 its likely someone will be.

Growing adoption of “Scorecards” to deliver security KPIs to businesses

Security teams and managers used to rue the fact that security wasn’t on the board’s radar. Then “cyber security” lifted the topic to that level and the result was often a poorly communicated list of technical challenges, litanies of control failures that were used to justify yet more controls and an increased volume of reports and assessment/scan/testing output. This basically all translated as “security isn’t doing an effective job” rather than “here are the challenges our business faces”

The rise of scorecard-based approaches move beyond technology-led reports and dashboards showing issues, to the presentation of KPIs around the processes of delivering security outcomes.

With the right KPIs on the right parts of the security operational lifecycle, early adopters are seeing a better match between risk exposures (or compliance requirements) and the delivery of an effective security service.

Where these can be aligned to business fundamentals like reputation or the bottom line then there is a much more obvious message that the risks to reputation or profitability are caused by a real risk of attack against identified critical systems.
We see scorecards and “management by KPI” becoming more normal in the security function; as a way to bridge the complexity of dealing with the challenges themselves, with the need to report on the progress that is being made.

Distributed AI attacks emerge

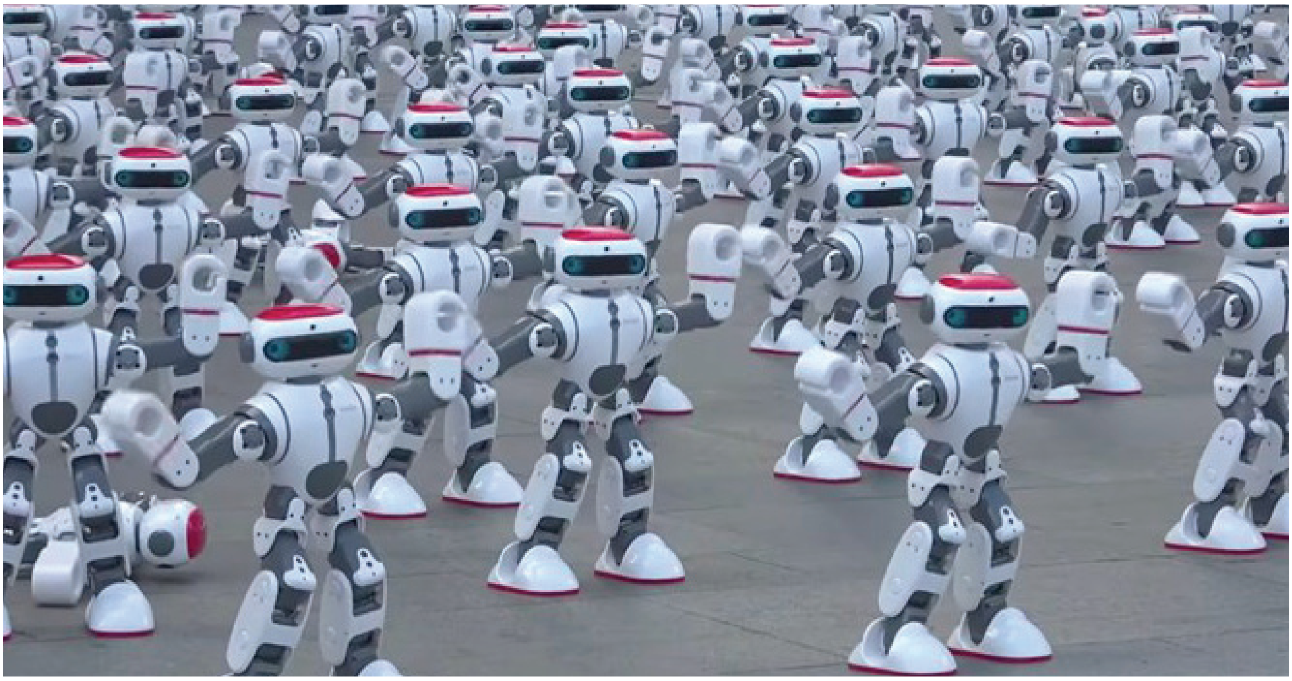
There has been an increase in the use of AI, machine learning and automation in security defence for a while now. Network and system activity monitoring often utilise these techniques as well as heuristic approaches to user behaviour and malware detection. Newer technologies that use machine learning to understand behaviour, and thus detect and understand anomalies are also available.

However, attackers have access to the same computers, the same algorithms and equivalently clever research. So we will see attack techniques that go beyond just trying to beat these advanced machine learning/AI-based defensive systems, ones that actually use these advances to shape and mount a successful intrusion. This is a significant difference.

An attacker's goal might well be to identify and exploit a particular type of user, or find a characteristic system based on the vulnerabilities it contains, or confirm what type of person might be prone to a certain type of attack. This information might not be something they then use, but actually sell on to some other party, and that's a pretty scary use of AI or machine learning as the ability to generate that data becomes magnified.

In the same way Facebook, Google and Amazon profile us to serve up adverts they think we'll respond to, we may see attackers profile people, systems or businesses so they can get us (or the technology we use) to respond to attacks in a way that maximises returns.

If an attacker knows a person routinely buys cycling equipment, what better way to extract their credit card number than with a cycling-themed special offer email in the run up to Christmas; or to watch where they shop and then ask them to confirm personal details relating to the delivery of an order they just watched them place. These might be contrived examples, but combining large volumes of data and AI can serve any motivation – good or evil.



Continued shift from compliance to risk management

Compliance is a powerful driver for security operational improvement and both project and ongoing investment. The alignment, or certification, to security standards and guidelines is a common way of establishing an information security management system (ISMS); starting at policy, standards and processes then providing a way for audited and assurance technologies to support oversight, the delivery of solid IT services and robust controls.

However compliance has always been quite a blunt instrument and has risked, or in some cases actually become, a spreadsheet-filling or box-ticking exercise where lists of controls/safeguards were applied to an environment due to their inclusion in a standard of predefined "best practice".

This approach is OK "on average" but there is no such thing as an "average" environment so the desire to chase a clean audit has sometimes meant businesses sidestepped risks they faced and just did "what it said on the tin" irrespective of the costs or impacts, because "compliance".

Prescriptive compliance approaches are now increasingly being replaced by a doctrine that business or system owners take responsibility for risks and make their own decisions about them. This is sensible as they can be more flexible, agree a lower or higher risk tolerance and apportion investment around the control set based on the threats faced by that specific business and its wider business priorities.

However, the stark reality is that often these decision-makers are not experts in cyber security or familiar with threats and methods of attack. Having been deprived of a clearly laid out list of things to do by a compliance standard, they can find themselves somewhat adrift between vendors of solutions, users of systems, a business trying to reduce costs and constant news stories about cyber threats.

Who would want their senior-level career exposed to those kinds of uncertainties when making decisions about a topic of which they have scant understanding?

However, this trend to risk-based decision making will continue in 2019, but it will not escape the underlying problem that cyber security is complex or that compliance provides at least one way to manage it.

Managed security services for SMEs

Smaller business often assume they won't be the target of a cyber-attack (through their size/scale or relatively low profile) and fail to invest accordingly. This decision is often based on very limited awareness of risk or a worrying lack of interest.

Even if a large number of small businesses suffer cyber-attacks, data losses or breaches, it may not be news even if the data involved, the nature of the businesses or the costs in each case make them individually significant. However, one major organisation suffering a breach, even with lower volumes of less sensitive data, can easily make the front pages.

The risk profile of an individual business can be irrelevant if an attacker simply casts their net as wide as possible and targets any vulnerable organisation – big or small.

When attack/exploit/phishing costs are as cheap as they have become, extracting 1 million records from one database or 1000 databases in 1000 record blocks is no different; in fact, for ransomware the very economics means that finding 1000 vulnerable smaller SME businesses that will pay a $500 ransom is preferable to betting on single organisation to part with $500,000 (which just won't happen).

The ability of SME's to mobilise the sort of skilled teams larger businesses have at their disposal means that the smart ones, those looking to survive a cyber-attack, are increasingly turning to managed security services to take on everything from simply administration of security controls, monitoring and operational oversight and then alert and incident detection, triage and response. The normalisation of this as an approach can only accelerate in the short term.

What do these predictions mean for security teams in 2019?

> “At a more sophisticated level there is still a drive for advanced analytics, AI and machine learning-based solutions in the cyber security market.”

Interestingly, several of these trends look to have parallel solutions for security teams; hence the ability (or impetus) to achieve visible and wide-ranging improvements may be within their grasp.

The drive for compliance around core security protections has not disappeared; in the utilities sector there are the standards driven by EU adoption of the NIS directive (albeit different at national and sector level), US C2M2 standards, GDPR (and other national equivalents), and the raft of Government and sector controls standards (for example PSD2-derived EBA standards for finance in the EU and the “Essential Eight” in Australia).

Alongside this, system or business owners taking on the responsibility for making their own risk decisions, means that there is a need for better understanding, more automatic implementation of basic “cyber hygiene” controls and clearer reporting for non-security stakeholders that use and show KPIs for security control effectiveness and performance.

At a more sophisticated level there is still a drive for advanced analytics, AI and machine learning-based solutions in the cyber security market. As these become more advanced, automated and better able to understand the environments into which they are connected, they will increasingly be able to take actions to respond in a more controlled and effective way. Hence, there are opportunities for businesses large and small to deliver a more appropriate threat detection and response capability to respond to a growing number of cyber threats and increasingly complex technology.

Between these two extremes – automatically assured cyber-hygiene and advanced, automated analytics - there are opportunities for managed security service providers. These providers will be able to deliver the necessary operational monitoring and reporting at scale very effectively for small and large businesses alike – plus will have the expertise to get the most benefit from the advanced, outward-looking and threat-aware analytics solutions.

Their focus on cyber security outcomes, also means they stand a chance of attracting and retaining staff to sit alongside automated technologies to take combined ownership of the security process of detection, triage, diagnosis, containment, resolution and clean up.

MSSPs themselves have requirements; service delivery means not just “effective cyber security” as a technical capability, but also recognition that ease of deployment, scalability, automation, repeatability and support for separate or multi-tenant policy and business domains is vital to deliver a service across a scalable portfolio of customers with their own networks.

As for our first prediction about the threat to elections; that seems to be happening by not just foreign powers and activities, but also by those in government or power themselves. Whether it is disinformation, misuse of data, questionable campaign financing or voter and boundary manipulation, there are undoubtedly more challenges to voting, electronic voting, registration or counting processes than just the ability of an election to withstand a concerted cyber-attack.

Huntsman®

HUNTSMAN | TIER-3 PTY LTD

ASIA PACIFIC

t: +61 2 9419 3200

e: info@huntsmansecurity.com

Level 2, 11 Help Street
Chatswood NSW 2067

EMEA

t: +44 845 222 2010

e: ukinfo@huntsmansecurity.com

7-10 Adam Street, Strand
London WC2N 6AA

NORTH ASIA

t: +81 3 5953 8430

e: info@huntsmansecurity.com

Awajicho Ekimae Building 5F
1-2-7 Kanda Sudacho
Chiyodaku, Tokyo 101-0041

AMERICAS

toll free: 1-415-655-6807

e: usinfo@huntsmansecurity.com

Suite 400, 71 Stevenson Street
San Francisco California 94105

huntsmansecurity.com linkedin.com/company/tier-3-pty-ltd twitter.com/Tier3huntsman