Cyber Security Predictions for 2016

Huntsman®
Defence-Grade Security Platform

Cyber security was never far from the news in 2015, and that is unlikely to change in 2016.

CURRENT TRENDS TO CONTINUE

Despite various initiatives to increase cyber security skills and awareness, the reality is that the shortage of expert resources is also set to continue to be a challenge. Equally the number, frequency, duration and severity of breaches will continue to trend upwards.

At Huntsman, we foresee a continuation of the spread of cyber-attacks to organisations and even industries that have not previously seen themselves as high-risk targets.

MORE BUSINESSES IN THE FIRING LINE

Government and the financial sector are obviously familiar with various kinds of sophisticated and targeted attacks but in the last few years we have seen Utilities and Critical National Infrastructure enterprises (CNI) in the firing line. The CNI sector has still got work to do in their cyber defence efforts according to a recent EU report, particularly their operational IT systems that are so critical.[1-2]

INCIDENTS WAITING TO HAPPEN IN THE CONNECTED SOCIETY

One of the other new technology trends looming is the rise of connected devices – wearable technology market, home automation, connected cars and the Internet of Things (IoT) are all booming.

In general, these devices are conceived by designers and manufacturers who are highly attuned to consumer needs. As a result they collect data, communicate automatically, make extensive use of cloud systems; yet security and privacy are not core considerations for these platform and device providers.

Awareness of the vulnerability of networks in the exploitation of these devices is a key first step in any IoT cyber defence strategy. This means only one thing – a greater attack surface for all of us, at home and at work. So at this point it would be wise to assume that in 2016 and beyond these technologies will start to be exploited as equally inventive attackers find ways to exploit them.

1 http://www.infosecurity-magazine.com/news/breach-notifications-eu-security/
2 http://www.v3.co.uk/v3-uk/news/2438244/eu-agrees-security-laws-that-will-force-firms-to-disclose-cyber-threats

THE WAR ROOM TO THE BOARD ROOM

There is increasing recognition at senior management and board levels that cyber security threats can result in direct as well as consequential and reputational costs depending upon how they are handled. As a result an increasing number of organisations will seek to leverage the skills and techniques used in the defence sector in their cyber efforts.

It is now recognised that no single vendor's suite of technologies provides the security panacea; but increasingly integrated security solutions that enrich and complement multiple sources of intelligence are key to cyber resilience. In 2016, enterprises will start to talk about how these highly integrated solutions can reduce their time at risk by using technology that correlates across information silos to confirm the presence of inappropriate activities which would otherwise have gone undetected.

QUANTIFYING CYBER RISKS FOR BUSINESS

As the commercial implications of cyber threats become recognised by business stakeholders there will be strong momentum to speed up the prioritisation and response to those risks according to their potential impact to the business. Business needs to understand and quantify the business implications of a security incident much faster than is currently possible. Information about the commercial implications of a compromised host must be as available to the business as the potential exposure from a credit risk.

This will force new thinking from solution vendors about the role of security technology, the way systems are monitored for attacks and the methods of response. In 2016 customers will seek technologies that deliver faster and more accurate security decisions so they can act on them more quickly.

REDUCING TIME AT RISK

It can take more than 200 days to identify a threat in your organisation and another 70 days to resolve it[3]. Technology limitations and the shortage of scarce security specialists mean that the importance and exposure of businesses to cyber threats is being increased. Decisions will have to be made around which issues get routed to an analyst, which get handled by a third party service provider and which are addressed through technology.

OVER-RELIANCE ON SCARCE RESOURCES

There is a significant mismatch between the volumes of machine generated threat intelligence delivered to analysts and the human scaled processes they employ to piece together the information to verify threats. This overreliance on analysts and their painstaking manual processes will exacerbate the pressure on the limited number of experts currently employed in the sector.

3 2015 Cost of Data Breach Study: Global Analysis, Ponemon Institute, May 2015

REENGINEERING INCIDENT RESPONSE

In 2015 trends shifted from multiple isolated devices delivering threat intelligence to analytics platforms for analysts to manually interpret security intelligence. In 2016 automating routine security operations elements will emerge to hasten the threat resolution process and free up experts to focus on more complex situations.

Process automation can, of course, be seen as a threat to the status quo. However, it can also be a means by which the Incident Management process can deliver a significantly more efficient and streamlined threat resolution process. Through close integration of machine based analyses with human intelligence and insight, a hybrid process that meets the speed and accuracy required from the cyber security sector will result.

Automatically quarantining an infected workstation is hard to justify when there is a meaningful likelihood that an alert is indeed a false alarm; but as the level of certainty around automated decisions increases so too is the likelihood that the next generation of automation will reduce reliance on the overworked security analyst.

Click here to explore how Huntsman Security can help reduce your Business's cyber risk profile.

Or visit us online at **huntsmansecurity.com**

Author: Peter Woollacott
Co-Founder and CEO, Tier-3

Peter Woollacott is the co founder and CEO of Tier-3 Pty Ltd (now trading as Huntsman Security), the software company that holds the patent for Behavioural Anomaly Detection and developed Huntsman® Intelligent Security.

He has 25 years' experience in operational and risk management with companies like Lend Lease, CBA, AXA, EDS, PWC and Bain International. Peter holds Masters Degrees in Applied Finance and in Business Administration, and lectures in executive post graduate education at Macquarie and Sydney Universities.

Peter may be contacted at
pwoollacott@huntsmansecurity.com

Please visit the Huntsman Resources page at **www.huntsmansecurity.com/resources** for White Papers, Compliance Guides, Solution Briefs and more resources by this author.

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

100 Pall Mall, St James
London SW1Y 5NQ

North Asia
t: +81 3 5809 3188
e: info@huntsmansecurity.com

TUC Bldg. 7F, 2-16-5 Iwamoto-cho,
Chiyoda-ku, Tokyo 101-0032

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