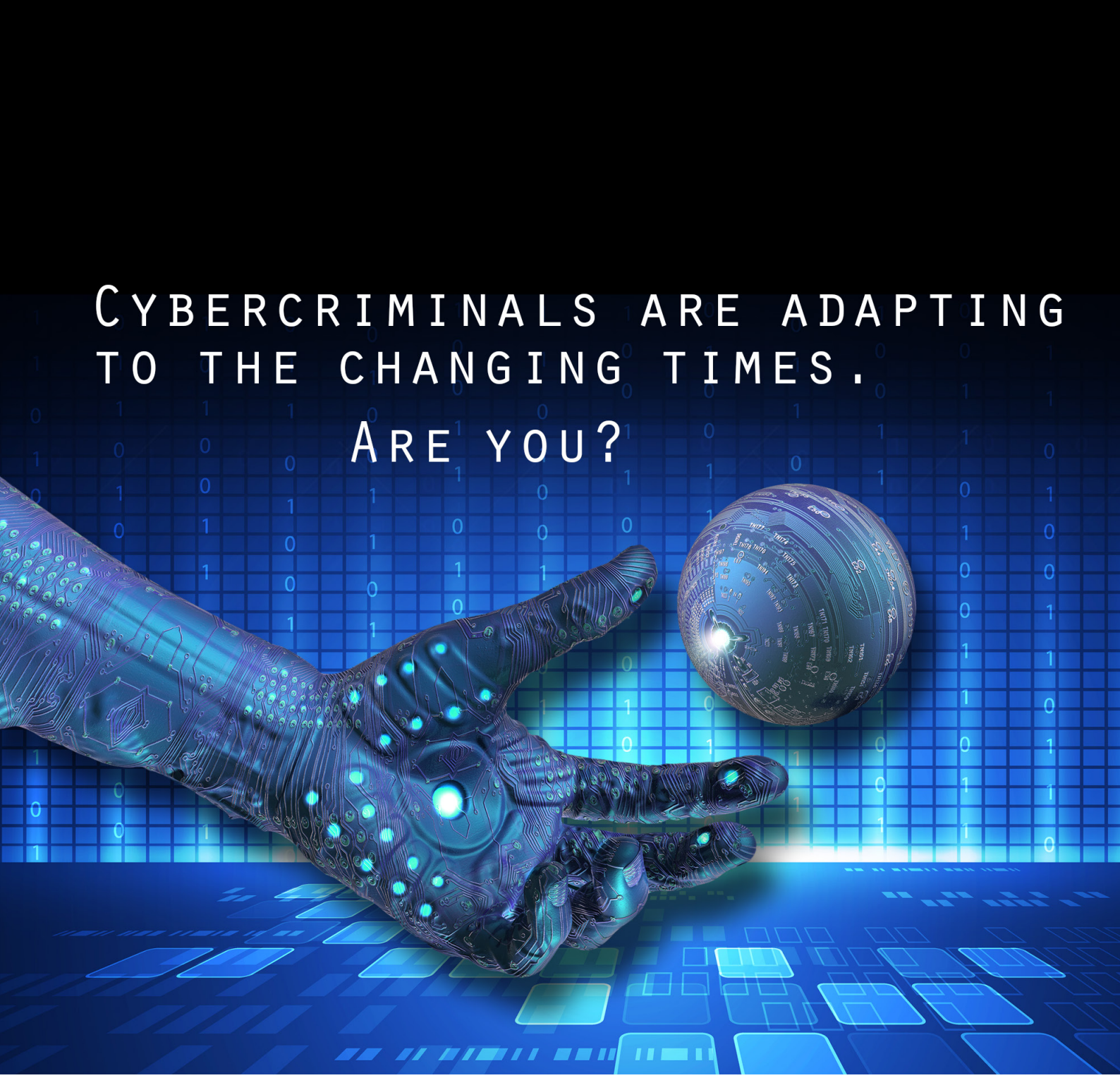
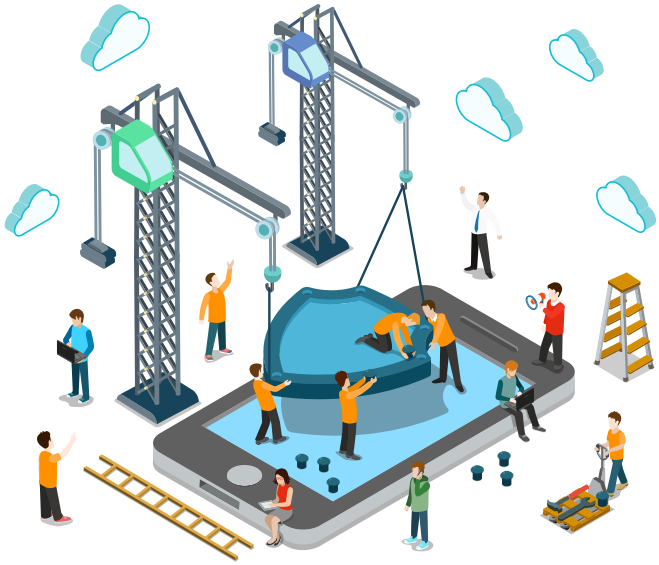
Cybercriminals are adapting to the changing times. Are you?



CSO
Custom Solutions Group

In partnership with ESET ENJOY SAFER TECHNOLOGY™



Cybercriminals are adapting to a changing world. And while that's obvious to the everyone working in security, ESETs Chief Research Officer Juraj Malcho wonders whether we are doing enough to adapt to a rapidly changing threat landscape.

During a recent CSO CXO Breakfast briefing, Malcho walked an audience of senior security executives through the local threat landscape, highlighting some of the most significant threats, and looked at what can be done to protect businesses and individuals.

One of the great advantages, says Malcho, of today's world is the richness of the data available to security managers. As well as the data available through SIEM platforms, Malcho noted the availability of threat intelligence data from many other sources.

From that data, it's possible to put together comprehensive views of what is happening in the world and predict what might happen in future. Malcho told the audience about how the use of some forms of malware can be accurately predicted as criminal gangs run regular campaigns on a reasonably predictable schedule where they target specific countries or industry verticals.

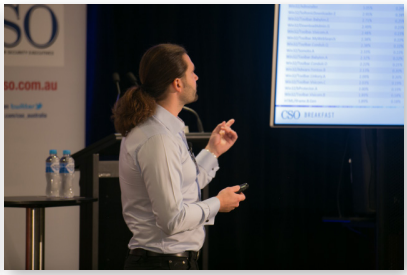
Furthermore, many threats seem to attack different industries sequentially. For example, manufacturers might be attacked first followed by retailers. For this reason, Malcho says it is important for security professionals from different industry groups to communicate and share intelligence.

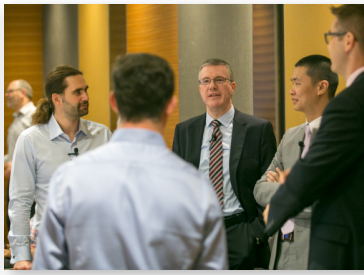
Unlike the early days of cybersecurity, broad-based threats are rarely the most significant issue businesses face. Malcho says "potentially unwanted software" that enters a business through a highly targeted attack is a more serious threat.

This software stays dormant on the network with the attackers tailoring the malicious payload to extract very specific information or to inflict maximum damage at a specific moment.

One of the great advantages, says Malcho, of today's world is the richness of the data available to security managers.

From that data, it's possible to put together comprehensive views of what is happening in the world and predict what might happen in future.





IoT threats

With organisations such as Gartner suggesting there will be in excess of 50 billion devices connected to the Internet by the end of the decade, the potential for criminals to exact all sorts of damage is significant. Malcho notes that companies releasing "Internet of Things" devices are making the same mistakes that were made when people started connecting devices to the Internet almost three decades ago.

"Time to market is the most important thing, not security," he says.

Companies releasing "Internet of Things" devices are making the same mistakes that were made when people started connecting devices to the Internet almost three decades ago.

The problem will become so prevalent that he expects people to start preferring 'non-smart' options as they become more concerned with the potential for attacks and increased maintenance costs associated with securing and updating more end-points.

Unlike many security experts, Malcho does offer a potential solution, suggesting two different classes of Internet of Things devices.

Malcho suggests that a class of devices is defined with a specified end of life where they stop functioning when their time elapses. The devices would not be updateable and would be extremely cheap – so cheap that replacement is preferred to remediating future issues.

More complex devices, such as cars, routers and other appliances, would be governed by a stricter set of rules – possibly backed by legislation and other legal frameworks.

"It doesn't make sense to treat all devices the same way," he says.

They're not APTs

Over the last few years, various security software companies have pointed to the rise of Advanced Persistent Threats, or APTs, as a significant issue. However, Malcho says this is the wrong way to look at these threats.

"Targeted Persistent Attack is much more spot on," he says. "Attackers combine different methods when doing reconnaissance – phishing phone call, targeting email borne malware to different people in an organisation".

This is because it's not the malware that is persistent but the attacker.


What can you do?

One of the criticisms often levelled at modern end-point protection is that it hasn't kept pace with modern threat. But Malcho says it has followed malware evolution through tools such as network communication inspection, emulation and sandboxing of analysed code, behavioural monitoring and memory scanning, stealth detection tools which can't be tested by malware writers and a gradual move from automatic to more verbose and interactive solutions.

But this is not without challenges. Trying to choose the right solutions can be a daunting task. Malcho says you can start by consulting with analysts or public testers but these might not be definitive and it's important to be aware of any potential bias.

For enterprises, this is further complicated. Internal testing is best but very difficult and your needs will probably go beyond detection with footprint, reliability, manageability, and support quality all critical.

The focus, says Malcho, is on focussing the defence to adequately cover your potential adversaries. And while he advocates combining different layers, he says it's important to not make it publicly known what security tools you are using.

As far as getting the c-suite engaged, it's critical to present the security discussion in business, rather than technical terms. During roundtable and panel discussions following Malcho's presentation, it was universally agreed by attendees that the information security discussion needs to be presented in terms of organisational risks and for the decision to spend on particular solutions be presented in financial terms where the cost of a breach is measured up against the cost of mediation.

Information security discussion needs to be presented in terms of organisational risks and for the decision to spend on particular solutions be presented in financial terms where the cost of a breach is measured up against the cost of mediation.

That means divesting some of the responsibility for security risk through the whole executive team and putting security-related KPIs into the performance plans of all managers with a responsibility for data integrity.

To find out more about ESET go to: http://www.eset.com/au/business/