RESILIENCE AND CYBERSECURITY STRATEGY

Jarno Salonen

YAKSHA Final end-user event

9th December 2020

Presentation Outline

What is resilience?

Top 2020 cyber threats

Today's complex model

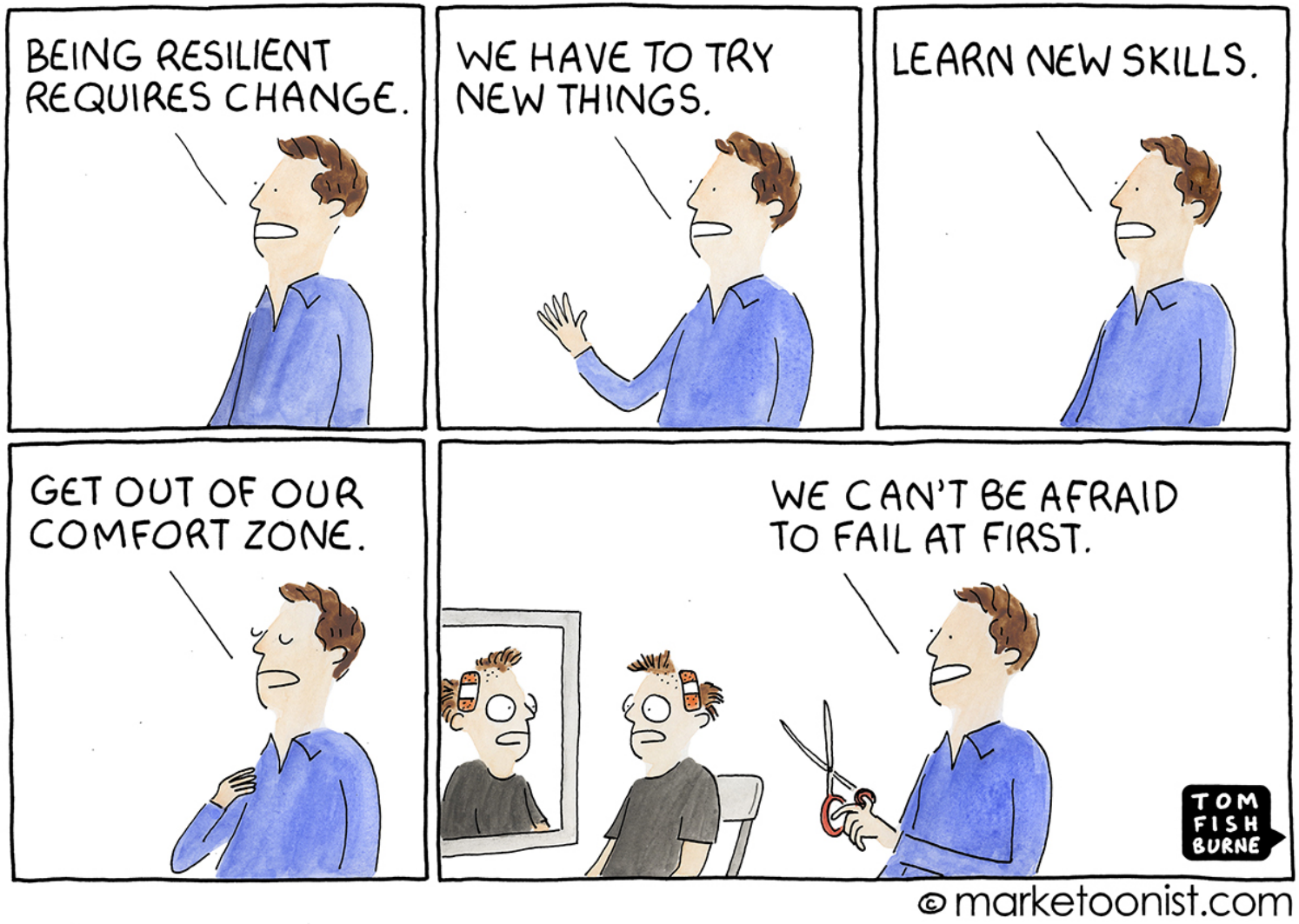
How to become cyber resilient

Keys to a good cyber resilience strategy

The other alternative

YAKSHA

What is resilience?



Definitions of resilience

"the capacity to recover quickly from difficulties, toughness"
"the ability of a substance or subject to spring back into shape, elasticity" *- Oxford languages*

"Resilience is the psychological quality that allows some people to be knocked down by the adversities of life and come back at least as strong as before" *-Psychology today*

"you make people resilient by exposing them to things that they are afraid of and make them uncomfortable voluntarily and use exposure…" *- Jordan B. Peterson*

"In computer networking, resilience is the ability to 'provide and maintain an acceptable level of service in the face of faults and challenges to normal operation' " *- ResiliNets Research Initiative*

"Cyber resilience is being able to prepare for, withstand, rapidly recover and learn from deliberate attacks or accidental events in the online world." – Scottish cyber resilience strategy 2015-2020

Top 2020 cyber threats

Phishing and business email compromise

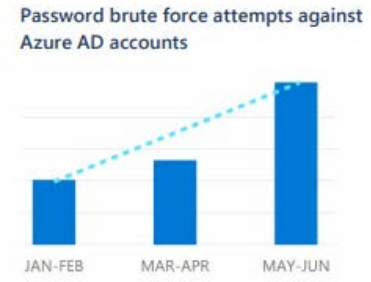
What we've seen in Office 365 Advanced Threat Protection detection in the past year:

6T	~13B	~1.6B	~1.7-2B
Messages scanned	Malicious emails blocked	URL-based email phishing threats blocked	URL payloads being created each month, orchestrated through thousands of phishing campaigns

Ransomware

> *In some instances, cybercriminals went from initial entry to ransoming the entire network in less than 45 minutes.*

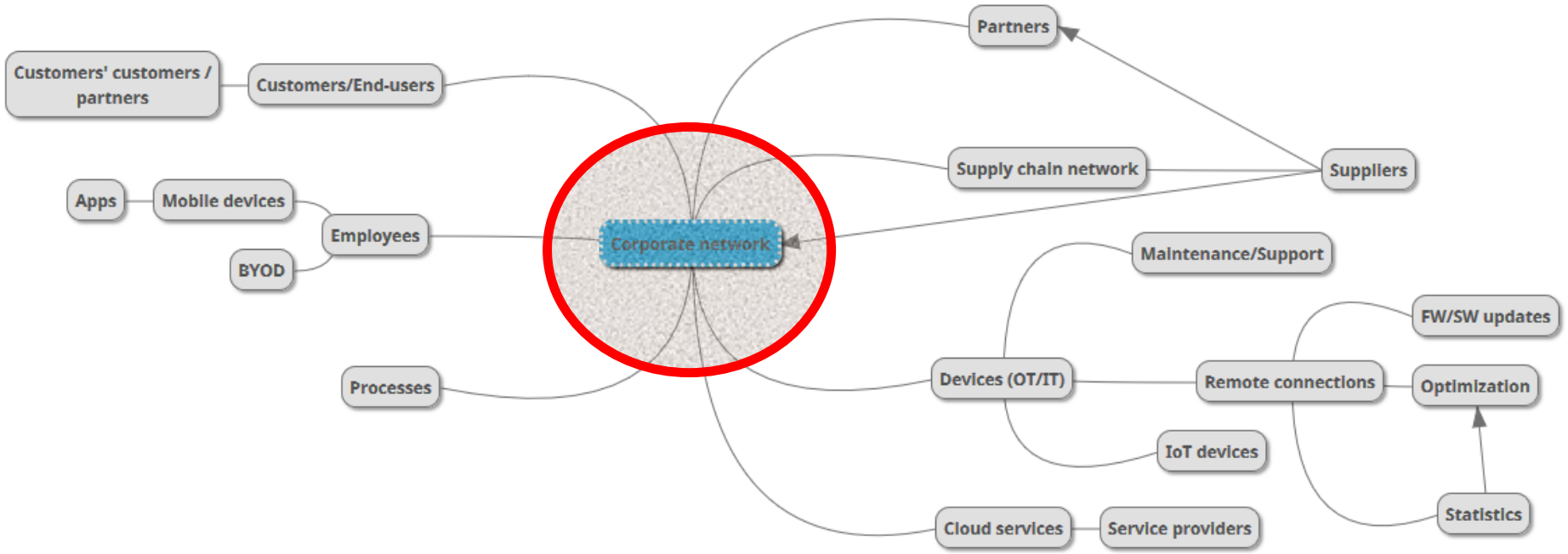
Identity and access management



Source: Microsoft Digital Defence Report, https://aka.ms./digitaldefense

Today's complex model

The paradigm shift from a protected corporate network into a combination of interconnected platforms, services and apps



How to become cyber resilient

Understanding your own assets/capabilities

- Core assets and their risks/threats
- Personnel and awareness
- Firewalls, other hardware/software
- Importance of updates
- ...

Knowing the environment that you are in

- Situational awareness
- Threat intelligence
- Following legislation and other relevant regulation
- Compliancy
- …

Preparing for the worst

- Defining security policies, measuring your security level
- Practicing incident and response, threat mitigation etc.
- Training personnel
- Sharing information and experiences
- …

46%

of security professionals claim that their cyber resilience is impeded by a **lack of visibility into applications and data assets.**

Source: https://resources.malwarebytes.com/files/2019/07/IDR-White-Paper_How-to-Become-Cyber-Resilient_FINAL_July-2019.pdf

Belgium/Netherlands/Luxembourg: One in four firms target of cyberattack in 2020 07.12.2020

A study by Trend Micro has shown that 76% of Benelux companies have been the target of at least one cyberattack in 2020. Less than 25% indicated that they had not suffered any cyberattacks that infiltrated their networks and systems in the past 12 months. Almost one in 10 companies surveyed say their networks and systems have been infiltrated more than 10 times. Just over 80% of Benelux firms reported that internal information was lost or stolen at least once, and two thirds say this was the case with customer data.

Source: https://www.lalibre.be/economie/digital/trois-organisations-sur-quatre-ont-ete-infiltrees-par-des-cyberattaques-l-an-dernier-5fc8f706d8ad5874796a7fcf (original French article)

Conclusion

CS V provided a realistic environment for our national cyber response apparatus to assess cyber incident response capabilities. DHS and participating organizations worked closely to establish the exercise's goal and objectives and design a realistic scenario that allowed stakeholders to address both organizational and national-level objectives. The resulting scenario allowed the community to coordinate a national-level response to a significant cyber incident. As part of exercise play, players identified significant findings and actions at the national, state, sector, and organizational level that the cyber response community should address. Ultimately, CS V served as a tool that allowed the stakeholder community to examine the evolution of cyber response capabilities and identify current gaps and challenges in responding to a coordinated cyber attack with global impacts. As a result, stakeholders have the opportunity to address these findings and bolster cyber response capabilities at an organizational-level, increasing the preparedness of the nation as a whole.

Source: https://www.cisa.gov/sites/default/files/publications/CyberStormV_AfterActionReport_2016vFinal-%20508%20Compliant%20v2.pdf

Keys to a good cyber resilience strategy

Digital transformation a.k.a. digital leap is inevitable

- Take into account all of the dimensions; business process, business model, domain and cultural/organisational

Cybersecurity is a key element of being resilient

- However you shouldn't focus on just technical cybersecurity measures in your strategy

Assume breach

- The question is no longer if a cyber attack will happen, but when – and how soon are you going to find it out?

Nurture an information-sharing culture

- Employees at high-performance organizations are four times more likely to share knowledge with their colleagues as workers at low-performance organizations

YAKSHA

The other alternative

Thank you for your attention!

Jarno Salonen
Connectivity solutions / Industrial cybersecurity
VTT Technical Research Centre of Finland Ltd
Email: jarno.salonen (at) vtt.fi

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 780498