Cyber Threats & Opportunities For Telecom Operators

Capacity Europe October 2017

Patrick Donegan

Founder & Principal Analyst, HardenStance Ltd

October 26th 2017

HardenStance

About HardenStance

- HardenStance delivers best in class research, analysis and insight in telecom and IT security.
- Founded in November 2016.
- Founder and Principal Analyst is Patrick Donegan, previously Chief Analyst, Heavy Reading.
- Also an Independent Analyst Contributor to Heavy Reading & Analysys Mason.
- Advisory Board Member, The Cyber Rescue Alliance

Agenda

1. The threat landscape
2. How telcos are faring
3. Embracing Software Programmability
4. Monetization
5. Preparing for the worst
6. Concluding Remarks

The New Threat Landscape

Then

Now

The Root Causes Of The IoT Security Problem Won't Be Solved – For Years

National Governments *Regional Trade Associations* *International Trade Agreements*

Consumer electronics vendors

Software developers

Component vendors

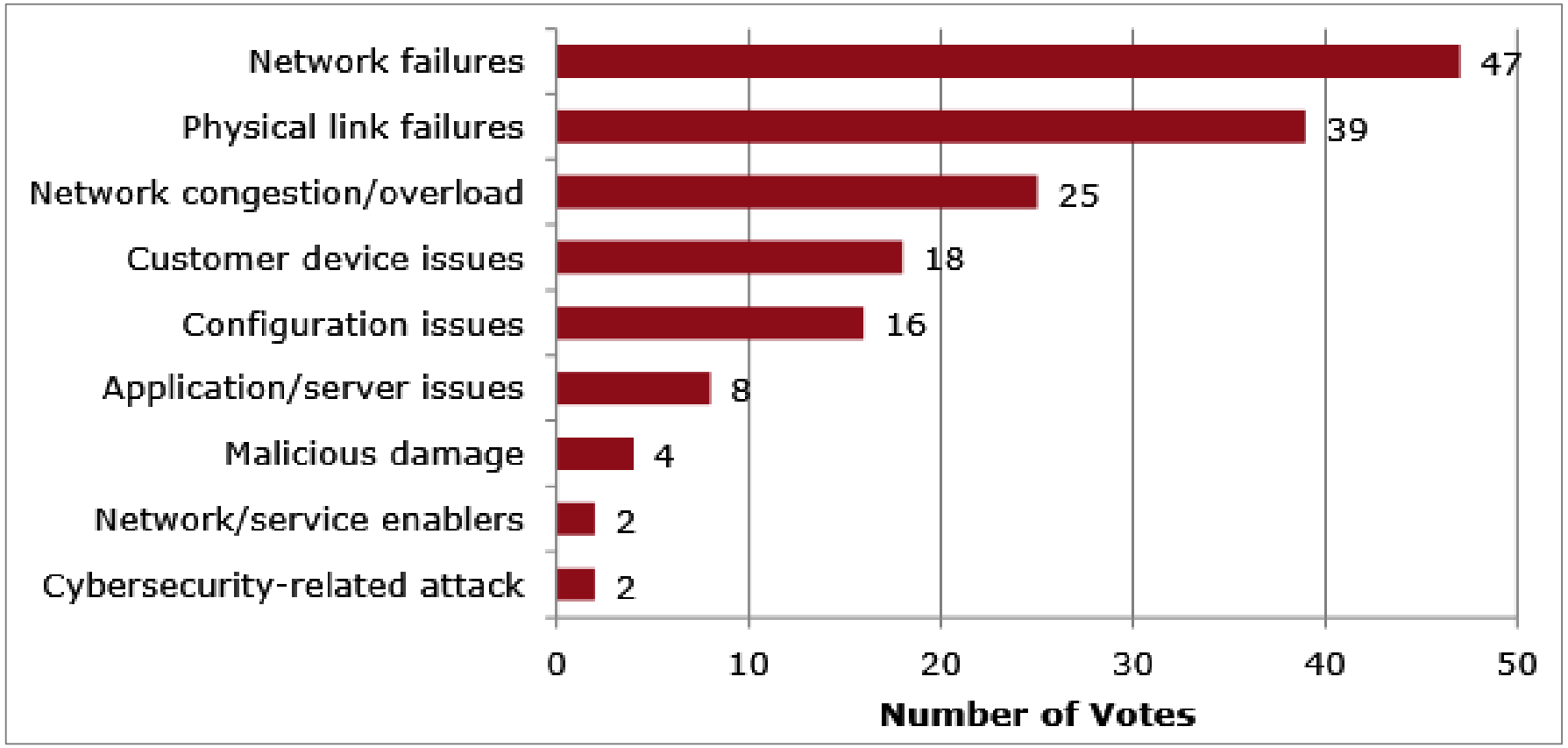
Consumers

Enterprises

Network providers

How Telcos Are Faring In The Threat Landscape

Most Common Causes Of Mobile Network Outages & Degradations



Source: "Mobile Network Outages & Service Degradations. A Heavy Reading Survey Analysis, February 2016 N= 54 service provider respondents

[Heavy Reading Mobile Network Outages Report]

TalkTalk

Telecom Operators Targeted by Iranian Threat Group

"**A quarter of the targets work in the telecommunications vertical;** Middle Eastern & North African mobile telephony suppliers feature heavily."

Source: SecureWorks Counter Threat Unit (CTU), October 2015

Customer Record Theft & Ransom

- February 13th 2017
- "3" Denmark
- 3,600 customer records verified to have been stolen by local police.
- Names, addresses and civil registration numbers (not bank information or pin codes)
- Attackers demanded "millions" not to publish.
- "3" chose to hand over to police and not pay the ransom.

Deutsche Telekom impacted by Mirai

- 5.00 p.m CET November 27th 2017 Deutsche Telekom DSL customers begin being taken-off line.
- 900,000 DSL routers impacted by the MIRAI botnet.
- A vulnerability in a feature allowing operators – and potentially other third parties as well – to remotely upgrade the device firmware.
- Deutsche Telekom rapidly applies packet filtering rules and issues a customer advisory.

O2 Germany Hit Via SS7 Vulnerability

The Register®
Biting the hand that feeds IT

DATA CENTRE SOFTWARE **SECURITY** TRANSFORMATION DEVOPS BUSINESS PERSONAL TECH

Security

After years of warnings, mobile network hackers exploit SS7 flaws to drain bank accounts

O2 confirms online thefts using stolen 2FA SMS codes

By Iain Thomson in San Francisco 3 May 2017 at 20:02 48 SHARE

Megafon & Telefonica impacted by WannaCry

Woman in 'ridiculous pain' has amputation postponed by cyber attack

15 May 2017 | England

Share

NHS cyber attack: Stevenage Lister Hospital postpones cancer treatment due to attack

By Matthew_MH | Posted: May 15, 2017

Lister Hospital, which is operated by the East and North Hertfordshire NHS Trust

IoT_Reaper

- IOT device vulnerabilities
- Beyond MIRAI, beyond default passwords
- Code exploits
- Easier recruitment than MIRAI
- No DDoS activity (yet)

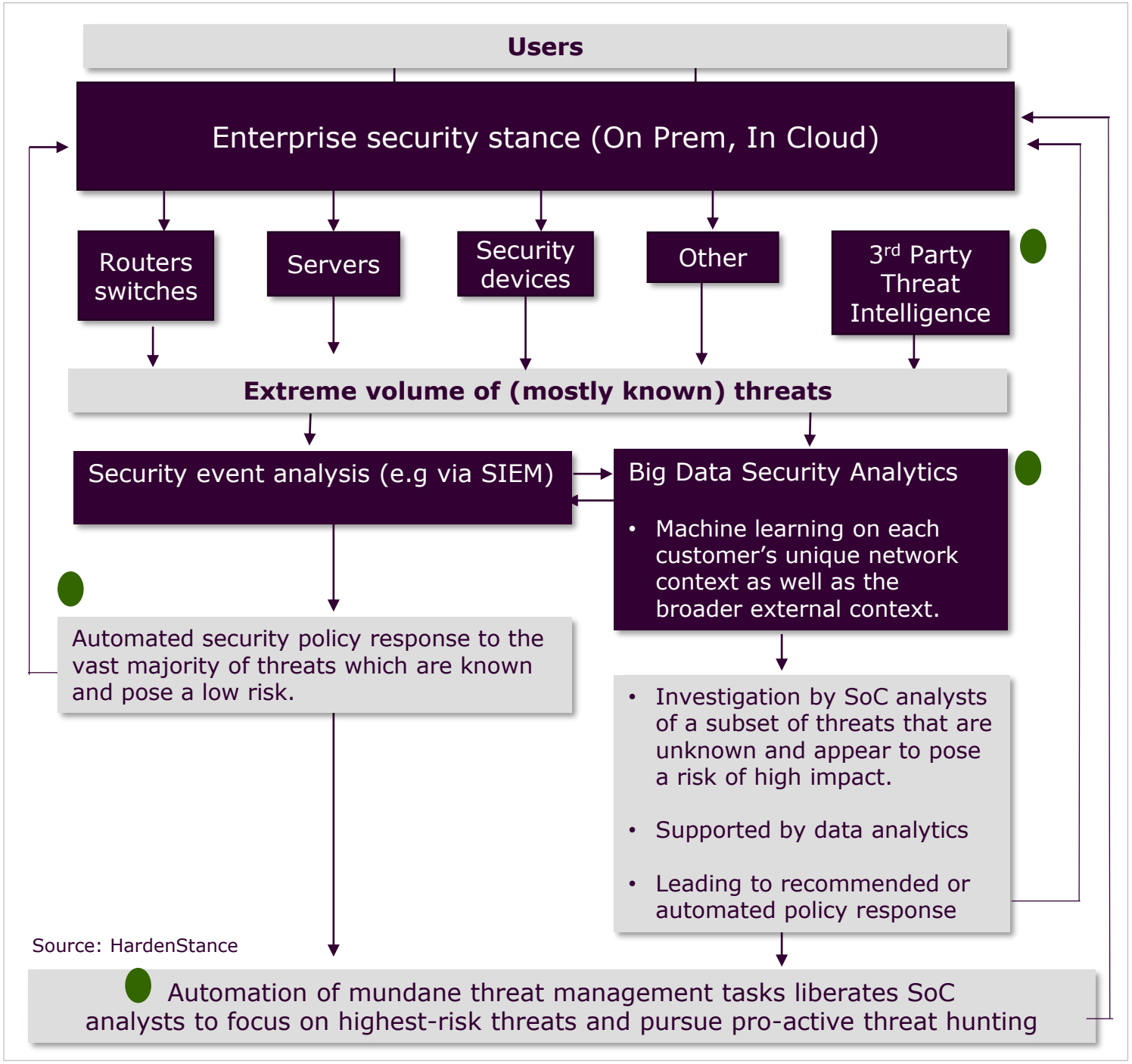
- Dlink (routers)
- Netgear (routers)
- Linksys (routers)
- Goahead (cameras)
- JAWS (cameras)
- AVTECH (cameras)
- Vacron (NVR

Embracing Software Programmability

Embrace Software Programmability

- Incremental progress with virtualization to date (5G looming)
- Centralizing security behind “the perimeter” doesn’t work
- Static security doesn’t work.
- “Explode, Offload, Reload” (© Ed Amoroso, Tag Cyber)
- Hypervisor Introspection & ETSI’s TEE for sensitive workloads
- Centralized policy with distributed enforcement.
- Security operations people are rightly wary of automation.

Embracing automation



CYBER THREAT ALLIANCE

Founding members

- Check Point Software
- Cisco Systems
- Fortinet
- McAfee
- Palo Alto Networks
- Symantec

Affiliate Members

- IntSights
- Rapid7
- RSA Security
- SK Infosec

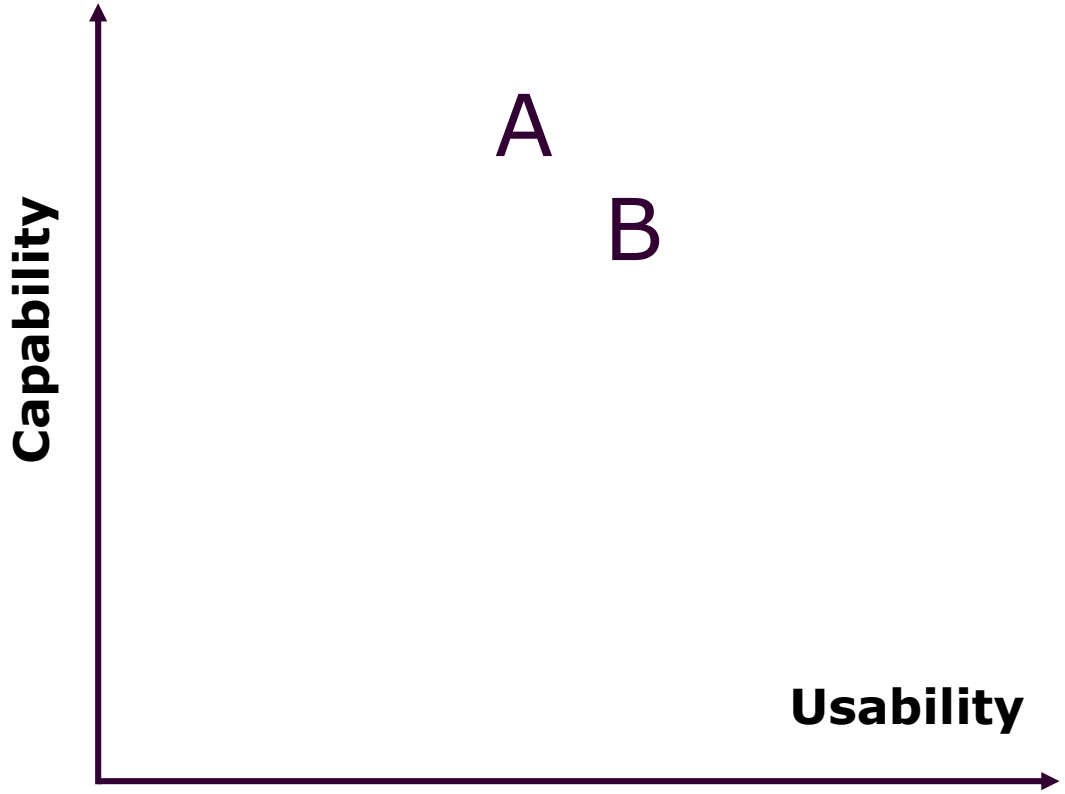
Contributing members

- Telefonica's Eleven Paths
- ReversingLabs

Source: Cyber Threat Alliance

HardenStance

Ease Of Use vs Performance Trade-Offs In Security Products



B is often Best

Planning for new security requirements is key…

…But don’t forget legacy vulnerabilities

SS7 migration outlook

3GPP TSG CT WG 3 Meeting 91 **C3-174370**
3GPP TSG CT WG 4 Meeting 79 **C4-174343**

Krakow (Poland), 21-25 August 2017

1 Overall description

CT3 and CT4 have concluded on the protocol selection for Service Based Architecture (SBA) of 5G core network for the Rel-15. The following conclusions are highlighted:

i. HTTP/2 (see IETF RFC 7540) is adopted as the application layer protocol for the service based interfaces;

ii. TCP (see IETF RFC 793) is adopted as the transport layer protocol;

iii. JSON (see IETF RFC 7159) is adopted as the serialization protocol;

iv To apply a RESTful framework for the APIs design whenever possible and use custom methods otherwise;

v To support notification with two HTTP client-server pairs;

vi The OpenAPI 3.0.0 is adopted as the Interface Definition Language.

The above conclusions apply for all the 5G core network interfaces under CT3 and CT4 remit which are defined as service based by SA2.

- HTTP2/TCP for 5G signalling
- Investment in Diameter for roaming
- (even) longer life for SS7?

Monetization

Security Vendor Sales (Year To June 2017)

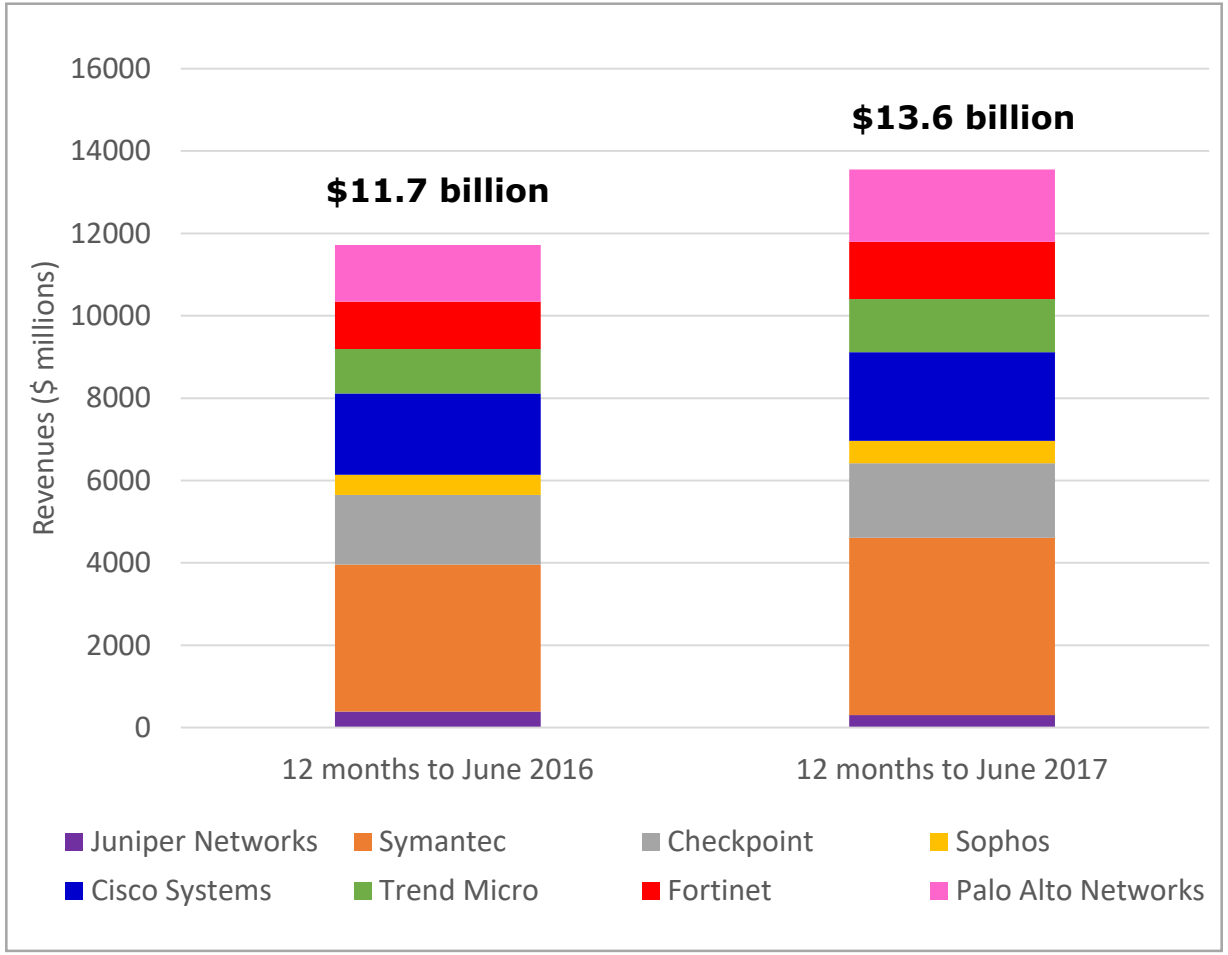
The HardenStance Network Security Spending Index (NSSI)

September 2017 Edition

Patrick Donegan
Founder & Principal Analyst, HardenStance Ltd

September 6th 2017

HardenStance



The eight security vendors generated total sales of $13.6 billion in the year to June 30th 2017, representing 15.6% sales growth over the year to June 30th 2016.

Monetization

[Analysys Mason Security For SMEs Report]

SME

National/regional corporate

Fortune 500

Preparing For The Worst:

Prepare for the impact of a major cyber attack getting through

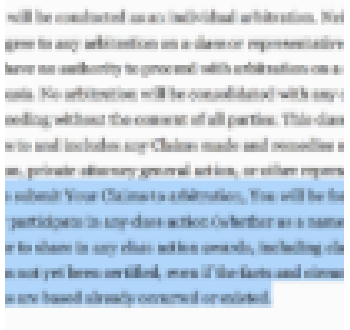
Preparing For The Worst – ***No, really***

EQUIFAX
PERSONAL
BUSINESS
GOVERNMENT
ABOUT US
PRODUCTS & SOLUTIONS
LEARN & SUPPORT
CREDIT REPORT ASSISTANCE
Equifax Cybersecurity Incident: To learn more about the cybersecurity incident, including whether your personal information
complimentary identity theft protection and credit file monitoring, click here
Your Credit, Your Identity.
Take control with a one-stop credit monitoring[1] and ID theft protection
solution from Equifax.
See your Equifax 3-Bureau credit scores in minutes
alerts about suspicious activities

Eric Schneiderman ✓
@AGSchneiderman

Follow

This language is unacceptable and unenforceable. My staff has already contacted @Equifax to demand that they remove it.



Zack Whittaker ✓ @zackwhittaker

PSA: If you check Equifax's site to see if your data was stolen, you *waive your rights* to sue Equifax or be part of a class action suit.

5:39 PM - 8 Sep 2017

The Emergency Breach Site

www.equifax.com

www.equifaxsecurity2017.com

www.securityequifax2017.com

The True Cost Of A Data Breach?

$350 million

YAHOO!

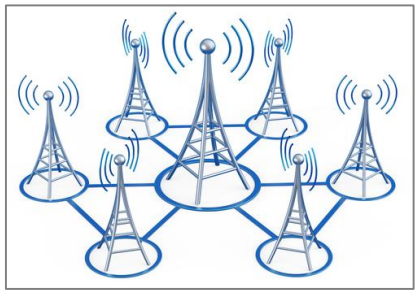
What was the outcome of your company's last cyber attack simulation?

What sections of your company's cyber attack response plan were subsequently amended?

Cyber Attack Simulation On An Affiliate Of A European Operator

The CYBER RESCUE Alliance

Phase 1



Phase 2

Phase 3

Learnings & Take-Aways

- HW bias
- Composition of teams
- Impact of phasing
- Deviation from plan
- Refinements
- Have a detailed plan.
- Have specialist resources to call on.
- This was a well-drilled tier one

See more here:

How Robust Is Europe's Telecom Sector Against Cyber Attacks?

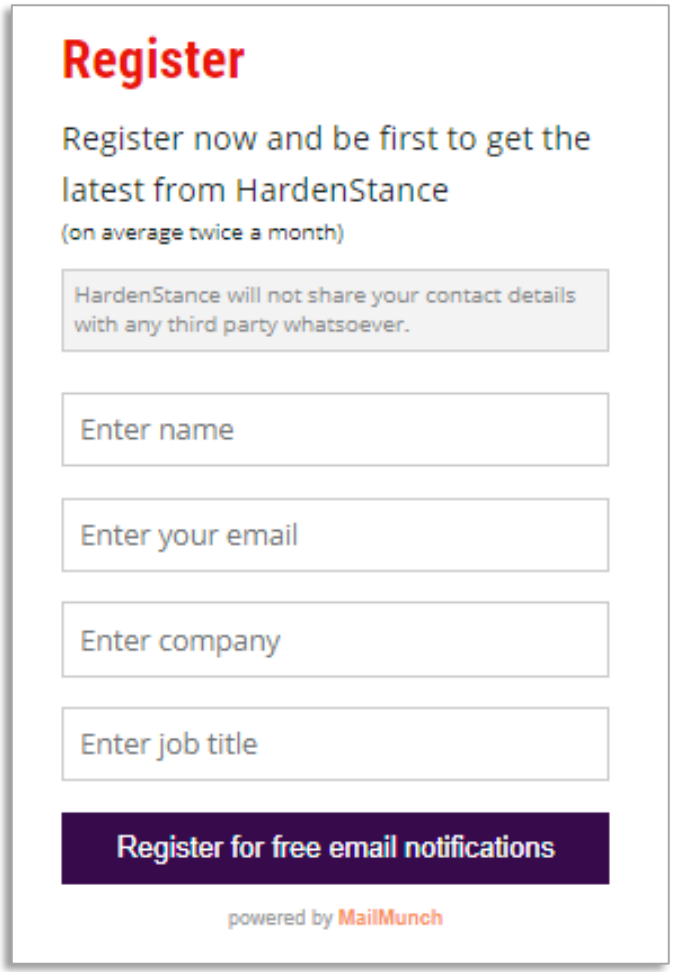
And here: https://www.cyberrescue.co.uk/

Concluding Remarks

- Take pride
- Learn
- Lean-In
- Monetize
- Prepare

…and if your main take-away from this talk is that the cyber threat landscape is ***"really scary"***….

Receive Email Notification Whenever HardenStance Publishes New Content



[Sign up for free email notifications here]

Thank you

www.hardenstance.com

patrick.donegan@hardenstance.com