ecosystm

THE PATH TO A CYBERSECURE ORGANISATION

Carl Woerndle
Cybersecurity – Incident Response & Recovery, Ecosystm

The Guardian

Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach

Whistleblower describes how firm linked to former Trump adviser Steve Bannon compiled user data to target American voters

- 'I made Steve Bannon's psychological warfare tool': meet the data war whistleblower
- Mark Zuckerberg breaks silence on Cambridge Analytica

Marriott hack exposes 500m guests

Starwood hotels data at risk • Passport and card numbers disclosed • Breach dates to 2014

HANNAH KUCHLER — SAN FRANCISCO
NAOMI ROVNICK — LONDON

As many as half a billion Starwood hotel guests may have had their private data stolen in one of the largest hacks in corporate history, which its parent Marriott International said exposed passport and credit card numbers.

Marriott, the world's largest hotel group, said it had learnt of the breach of Starwood's guest reservation database in September but that a subsequent investigation found the "unauthorised access" dated back to 2014.

The hotelier said about 327m of the 500m customers affected had some combination of their name, mailing address, phone number, passport number, Starwood preferred guest reservation number, date of birth and other identifying information exposed.

While payment card numbers and expiration dates held on the database were encrypted, components needed to decrypt this information may have been "taken" in the attack, Marriott added.

"We fell short of what our guests deserve and what we expect of ourselves," said Arne Sorenson, chief executive. "We are doing everything we can to support our guests, and using lessons learned to be better moving forward."

The data breach appeared to be the largest since Yahoo disclosed last year that more than 3bn of its users were hacked in 2013. The New York attorney-general's office said it was opening an investigation into the hack, but Marriott could be more vulnerable in the EU, where a new data protection law could leave it open to millions of dollars in fines. Marriott said it believed it had complied with the reporting requirements under the new law.

The hack would be by far the largest since the EU law came into effect in May. The Information Commissioner's Office in the UK, where Marriott's European operations are based, said it was "making inquiries". Marriott shares fell 6.3 per cent in late New York trading.

Marriott, the largest hotel group, says the full extent of the 'unauthorised access' to its database was realised only last week

Marriott, which bought the Starwood chain in 2016 for $13.6bn, said that while the breach had been detected in September, the extent of the problem had been determined only last week.

Jason Hill, lead researcher at CyberInt, a company that monitors the dark web, said he had not seen Marriott customer data on any of the websites he tracks. "With that amount of stolen data . . . it has great resale value on the underground economy," Mr Hill said.

Additional reporting by Camilla Hodgson

ABC NEWS

Just In | Australia | World | Trump's America | Business | Sport | Arts | Analysis &

Print | Email | Facebook | Twitter | More

Red Cross Blood Service admits to personal data breach affecting half a million donors

HELPNETSECURITY

art | News | Articles | Malware | Reviews | Events | Newsletter

DON'T MISS: Joomla users: Update immediately to kill severe SQLi vulnerability

Related topics

Microsoft patched the flaws allowing leaked Windows exploits to work

Featured news

Joomla users: Update immediately to kill severe SQLi vulnerability

WannaCry is a painful reminder of why enterprises must stay current on software updates

WannaCry: Smaller businesses are at great risk

Zeljka Zorz - Managing Editor
April 24, 2017

Tens of thousands Windows systems implanted with NSA's DoublePulsar

Read the latest issue of the (IN)SECURE Magazine

Has your Windows machine been implanted with NSA's DoublePulsar backdoor? If you haven't implemented the security updates released by Microsoft in March, chances are good that it has.

THE VERGE

TECH | SCIENCE | ENTERTAINMENT | MORE

APPS \ MOBILE \ TECH

Twitter advising all 330 million users to change passwords after bug exposed them in plain text

There's apparently no evidence of any breach or misuse, but you should change your password anyway

By Chaim Gartenberg | @cgartenberg | May 3, 2018, 4:21pm EDT

SHARE

distribute.IT

WHO WE ~~ARE~~ WERE

FORMED AS A STARTUP IN

2002

WEB SERVICES PROVIDER

Domain name registrar

Web/Server Hosting

SSL Products

SMS messaging

~10%

MARKET SHARE – .AU DOMAIN NAMES

30+

EMPLOYEES

OFFICES IN

Melbourne **Jakarta**

200,000+

DOMAIN NAME CLIENTS

30,000+

HOSTING CLIENTS

8-10 million

SMS MESSAGES PER ANNUM

3000+

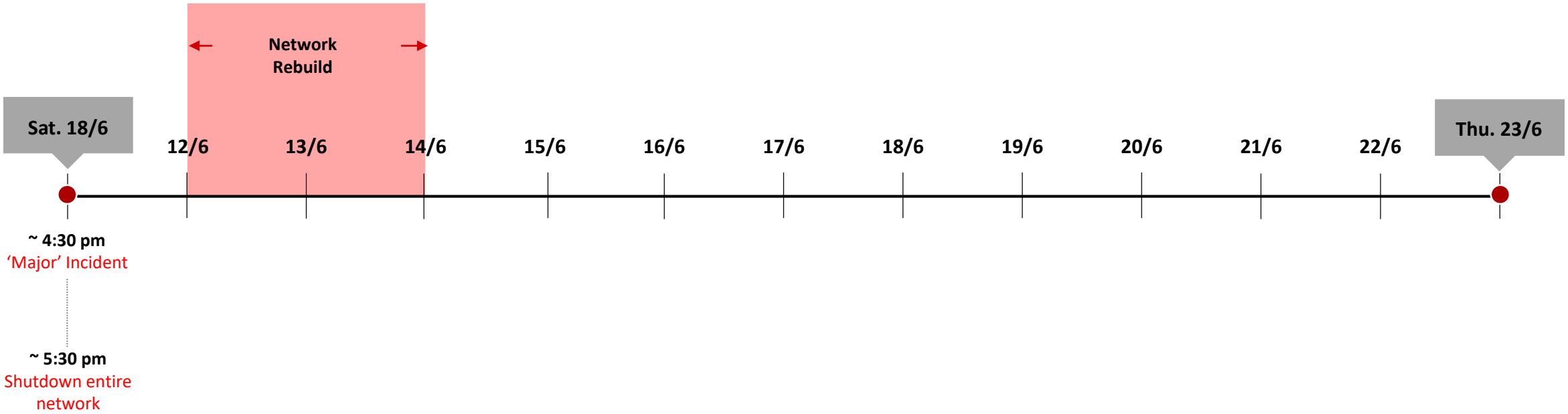
RESELLERS

BUSINESS WAS

Profitable **Cash Flow Positive** **Growing**

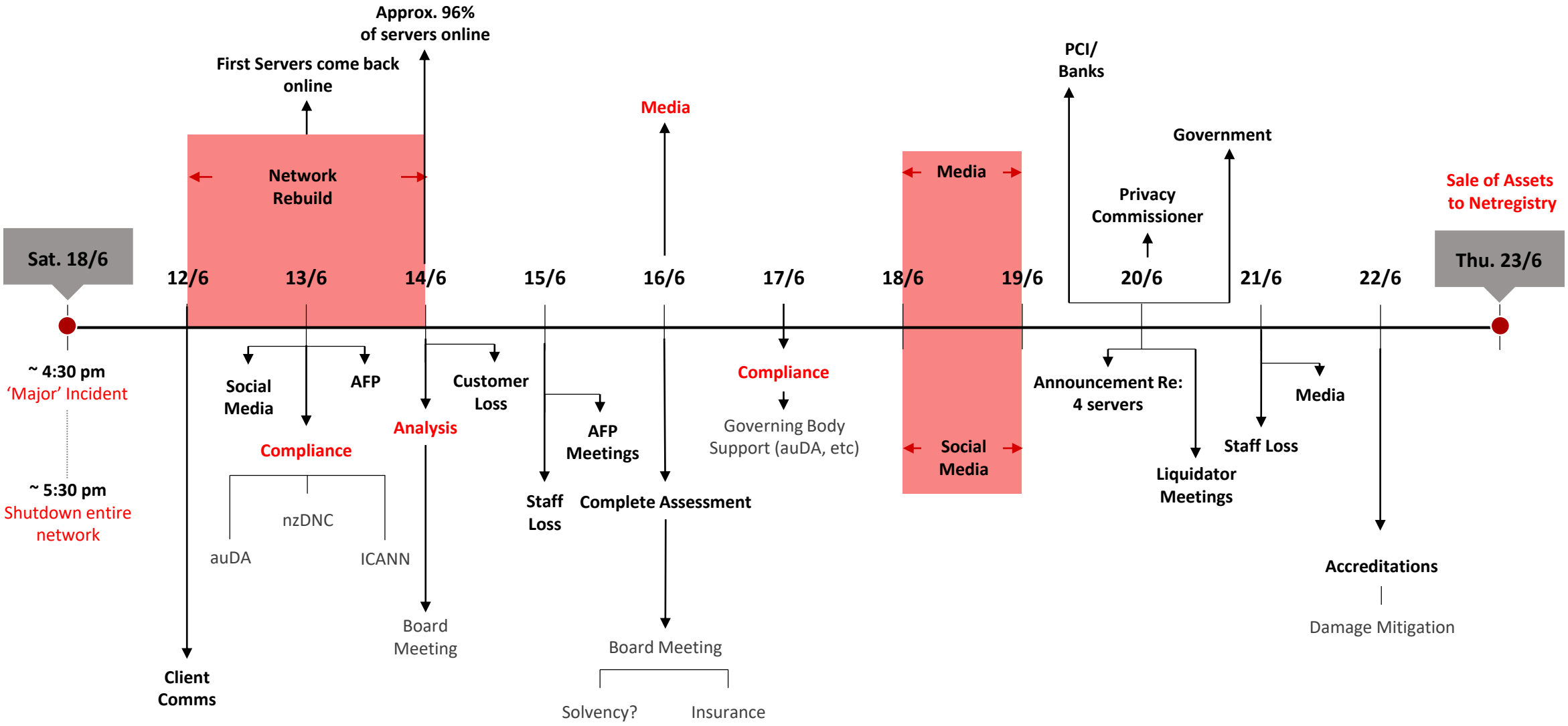
distribute.IT

MAJOR BREACH (11TH – 23RD JUNE, 2011)

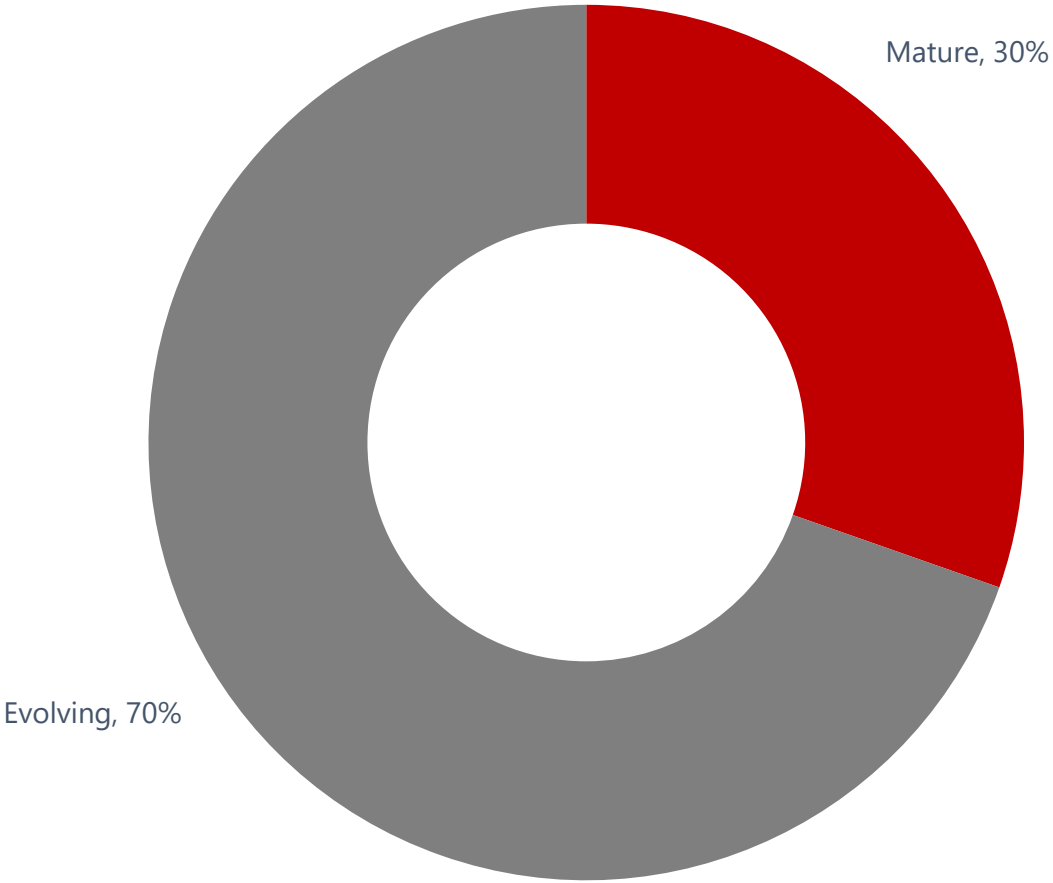


distribute.IT

MAJOR BREACH (11TH – 23RD JUNE, 2011)



THE DIFFERENCES IN CYBERSECURITY APPROACH



DRIVERS OF SECURITY INVESTMENTS

CHALLENGES OF IMPLEMENTATION

KEY SECURITY STAKEHOLDERS

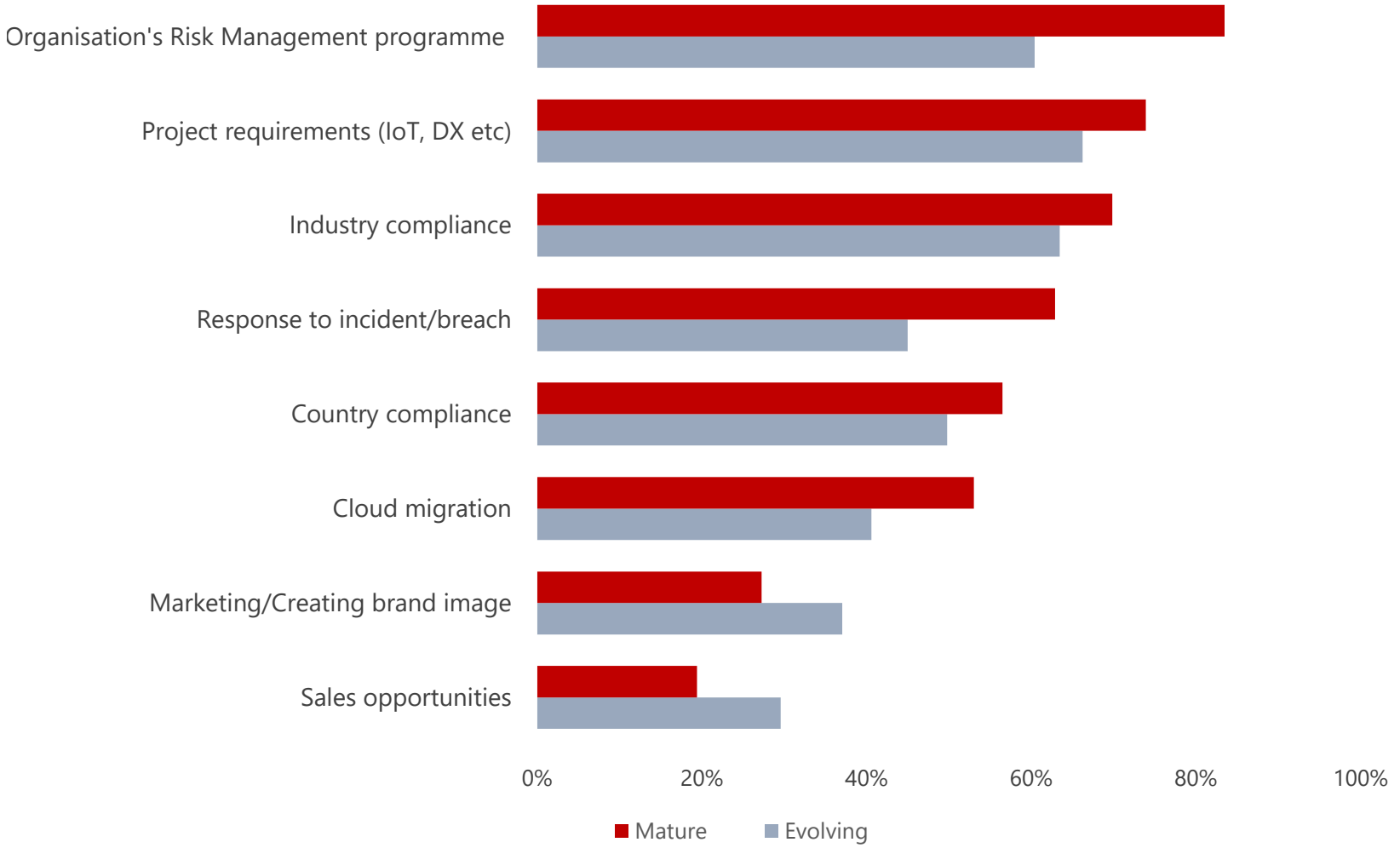
DATA CLASSIFICATION

BREACH HANDLING PROCESSES

** Mature : Organisations that rate the maturity of their Security solutions at an 8 or above (Scale 1-10)*

N = 1,136
Source: Ecosystm, 2019

#1 THE RIGHT MOTIVES FOR CYBERSECURITY INVESTMENTS



>75%

DON'T KNOW WHERE TO START OR WHERE TO FOCUS RESOURCES

Breach Prevention

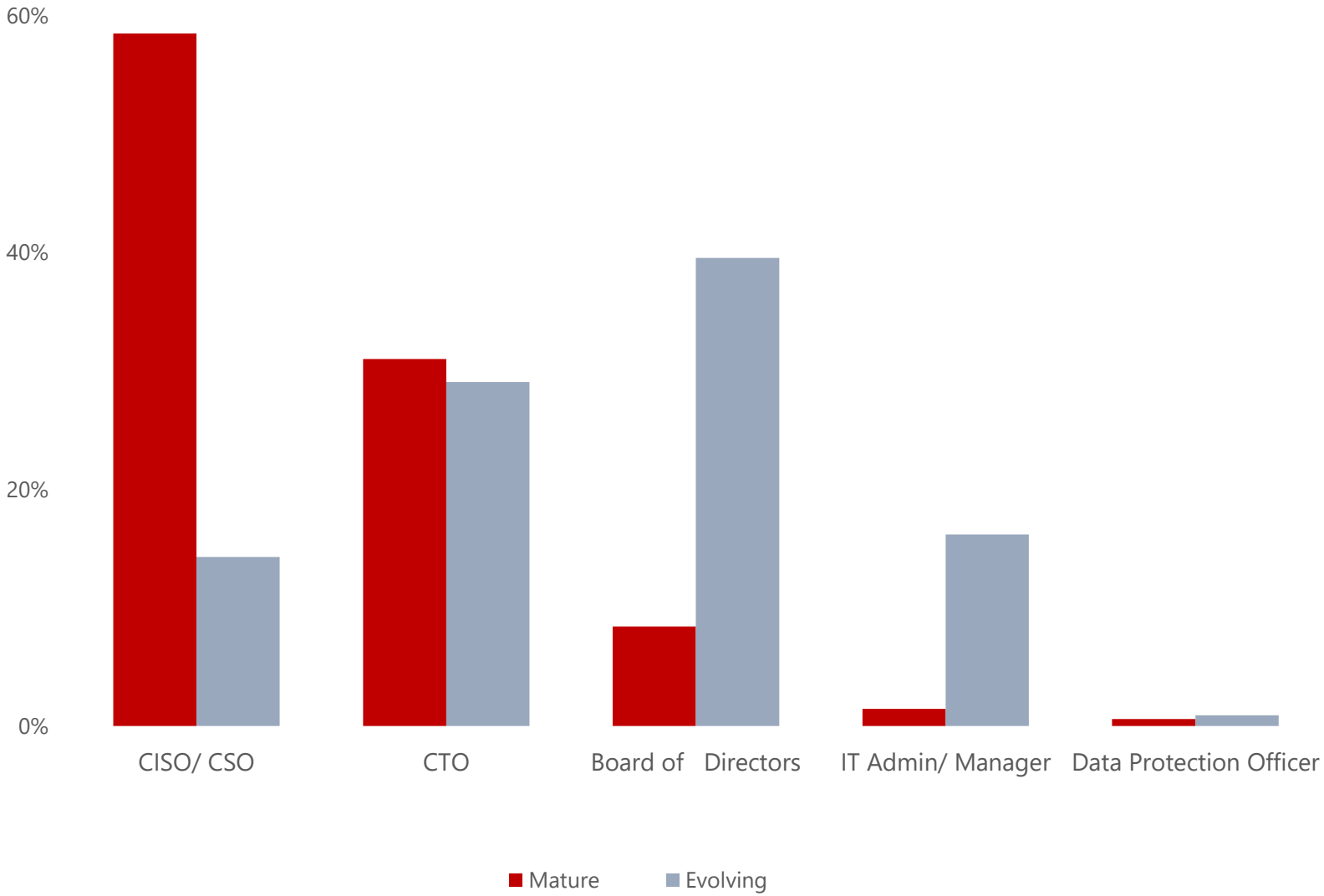
STARTING POINT OF SECURITY ROADMAP

Currently Focused On Compliance

UNCLEAR OF WHAT "RISK MANAGEMENT" ENTAILS

N = 1,136
Source: Ecosystm, 2019

#2 A DEDICATED FOCUS ON SECURITY



68%

OF EVOLVING ORGANISATIONS HAVE NO DIRECT RESPONSIBILITY FOR SECURITY

Engaging a 3rd Party Advisory firm

69%
MATURE

25%
EVOLVING

N = 1,136
Source: Ecosystm, 2019

#3 STARTING THE JOURNEY WITH DATA CLASSIFICATION

<50%

NOT IDENTIFYING KEY SENSITIVE DATA BEYOND IP & LEGAL

"General Data"

COULD STILL INTEREST HACKERS - AND ACT AS AN ENTRY POINT

N = 1,136
Source: Ecosystm, 2019

#4 AWARENESS OF CLOUD RISK

AVERAGE APAC ORGANISATION HAS

3 current cloud solutions

EXPECTED TO BE

5 by 2020

Store sensitive data on Public Cloud

31% MATURE

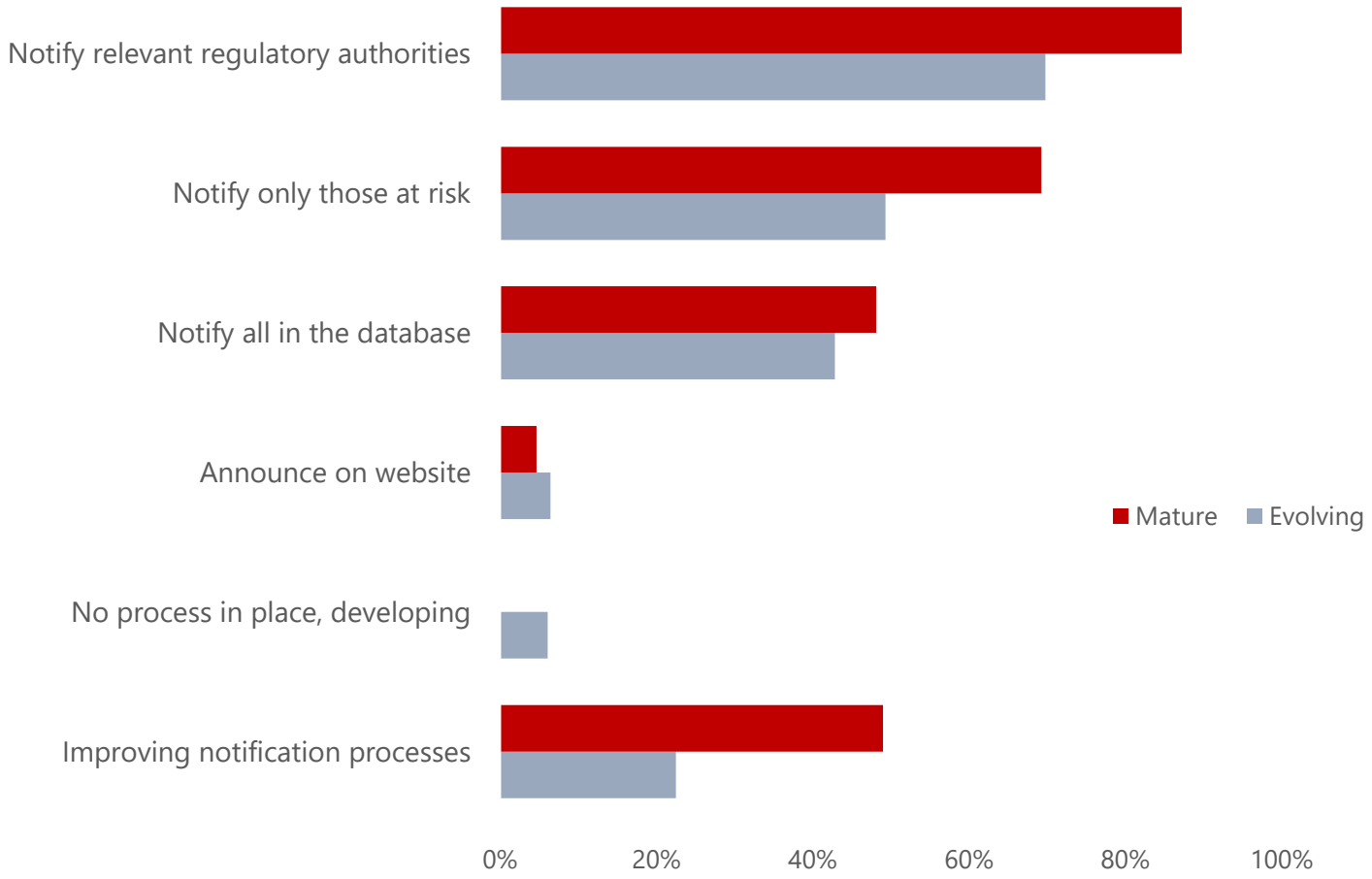
60% EVOLVING

Feel Public Cloud security features are sufficient

27% MATURE

56% EVOLVING

#5 READINESS TO HANDLE A BREACH



95%

NO BREACH/ UNSURE

73%

WHO CLAIM NO BREACH - SAY A BREACH IS INEVITABLE

Cybersecurity Insurance

70%

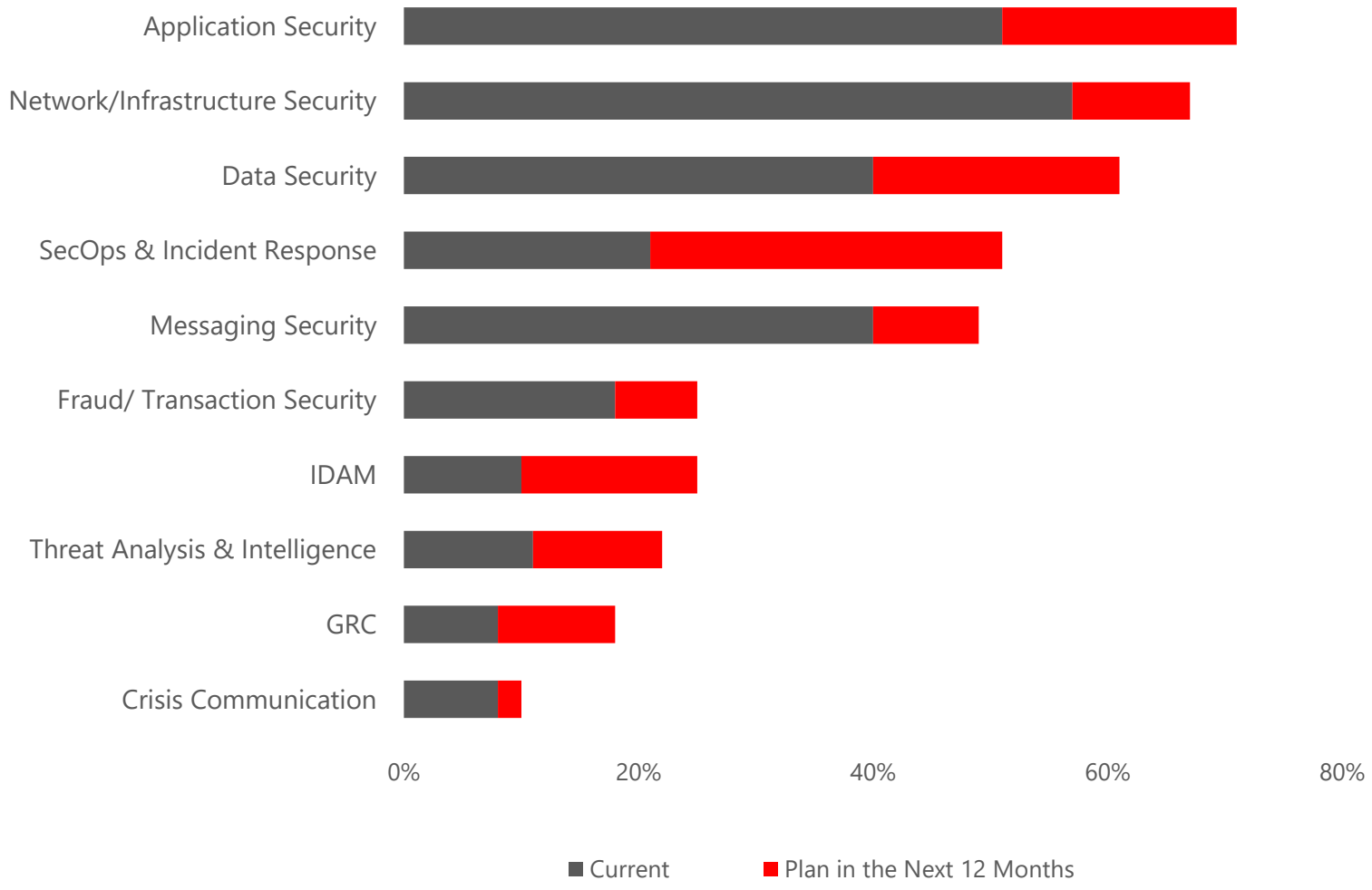
MATURE

33%

EVOLVING

N = 1,136
Source: Ecosystm, 2019

AND FINALLY… INVESTING IN THE RIGHT SOLUTIONS?



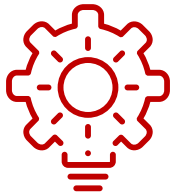
SHIFT OF FOCUS ON THE DATA AND NOT JUST THE PERIMETER

N = 1,477
Source: Ecosystm, 2019

KEY TAKEAWAYS

80% OF ORGANISATIONS CONSIDER THEMSELVES IMMATURE

Most still don't even know where to start



TECH BUYERS NEED TO BE PROACTIVE

Don't let an incident or compliance drive your security programme

CYBERSECURITY VENDORS NEED TO HELP ORGANISATIONS GO BEYOND "SECURITY AS A COST"

Understand the **real risk** and the value of a **structured** programme

ecosystm

THANK YOU

Carl Woerndle
Principal Advisor
carl.woerndle@ecosystm360.com