Understanding the Changing Cybersecurity Problem

Keith Price

BBus, MSc, CGEIT, CISM, CISSP

Founder & Principal Consultant

Copyright © 2018 Black Swan Consulting Group Pty Ltd

About

- About me
  - Specialise in information security strategy, architecture, and assessment
  - 30-year career in networking and telecommunications, the emergence of the Internet, Internet banking, and IT security
  - Work experience in AU, US, UK, Europe
  - BBus, MSc, CISSP, CISM, CGEIT

- About Black Swan Group
  - Professional services company in Sydney
  - Clients include financial services, education, not-for-profits, state & federal government, property management, and others.

Copyright © 2018 Black Swan Consulting Group Pty Ltd

All images not created by the author are used under the “fair use for education” provision.

Copyright © 2018 Black Swan Consulting Group Pty Ltd

Agenda

- A (very) brief modern history of ‘cyber’
- Scale of the cyber problem
- Clarifying cyber risk through attackers, vulnerabilities, & consequences
- Thoughts about cybersecurity
- Cybersecurity assessment

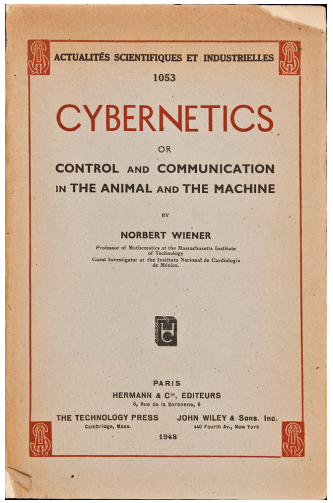
Copyright © 2018 Black Swan Consulting Group Pty Ltd

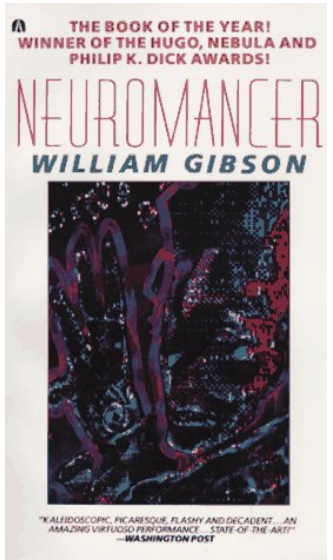
What do we mean by ‘cybersecurity’

Cyber is derived from cybernetics, the 1948 study of communication and control systems in living beings and machines.

Cyber can be added to (almost) any word to create an Internet reference (cybersecurity, cyberspace, cybercrime, cyberwar).

‘**Cybersecurity**’ has emerged as a single catch-all word meaning ‘trying to stop criminals attacking your IT systems to steal information or plant ransomware’.





Images: Google Images

Copyright © 2018 Black Swan Consulting Group Pty Ltd

The cyber risk problem

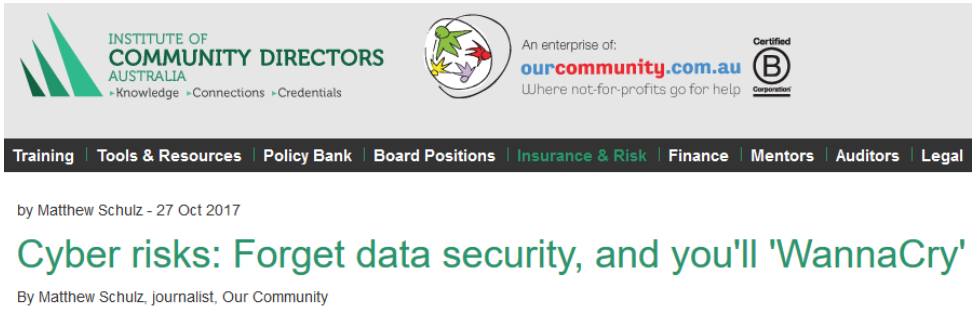
- Senior management thinks it's an IT problem (it's not).
- Every company is under constant attack, certainly by chance, other times a direct target.
- We are predictable because attackers know human weaknesses and the technologies we use.
- Their offence is easier and less expensive than our defence.
- Their offence just has to get lucky once. Our defence must be lucky always.

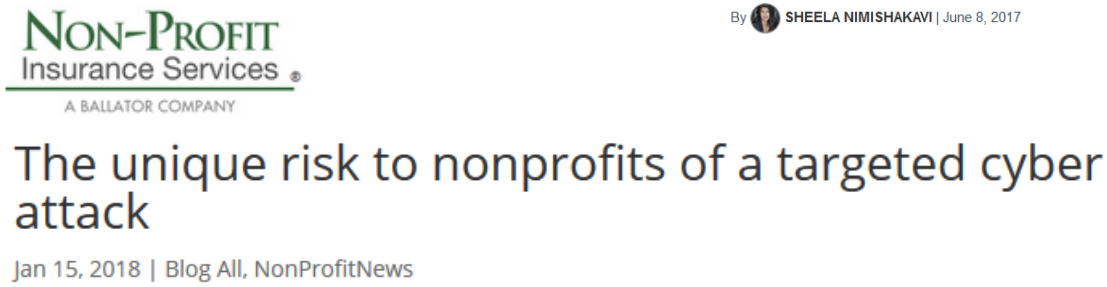
Leadership is the single most important factor in cybersecurity protection

Image: Google Images

Copyright © 2018 Black Swan Consulting Group Pty Ltd

Cyber risk to not-for-profits





Cyber risk is a board risk

news.com.au

Sony films boss Amy Pascal admits she was fired over leaked emails

FEBRUARY 13, 2015 5:44PM

Target fired CEO Gregg Steinhafel, cut compensation, proxy shows

Airplane parts maker fires CEO after he lost $56 million of company money in an email scam

Talktalk Telecom Group PLC
LON: TALK - 30 Aug., 4:47 pm GMT+1

199.54 GBX 0.00 (0.00%)

1 day | 5 day | 1 month | 3 months | 1 year | 5 years | max

Open	-	Mkt cap	1.82B
High	-	P/E ratio	32.99
Low	-	Div yield	-

100,000 customers left and a financial loss of £60M

CEO fired after 'fake CEO' email scam cost firm $47m

Liam Tung (CSO Online) on 26 May, 2016 09:29

Yahoo's head lawyer is taking the fall for its hacking, while CEO Marissa Mayer is getting her pay docked

Copyright © 2018 Black Swan Consulting Group Pty Ltd

Scale of the problem

Australia's relative wealth and high use of technology such as social media, online banking and government services make it an attractive target for serious and organised criminal syndicates. Lucrative financial gains by serious and organised crime syndicates ensure the persistence of the cybercrime threat.

The Cyber Security Review, led by the Department of the Prime Minister and Cabinet, found that cybercrime is costing the Australian economy up to $1 billion annually in direct costs alone. Cybercrime is diverting funds from the legitimate Australian economy to the illegitimate economy. In addition to loss of money, cybercrime causes other damage including:

- damage to personal identity and reputation
- loss of business or employment opportunities
- impact on emotional and psychological wellbeing.

AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION

Copyright © 2018 Black Swan Consulting Group Pty Ltd

Your biggest cybersecurity risks

1. Damage to reputation/brand
2. Economic slowdown/slow recovery
3. Increasing competition
4. Regulatory/legislative changes
5. Cyber crime/hacking/viruses/malicious codes
6. Failure to innovate/meet customer needs
7. Failure to attract or retain top talent
8. Business interruption
9. Political risk/uncertainties
10. Third party liability (inc. E&O)

Source: Aon Global Risk Management Survey 2017

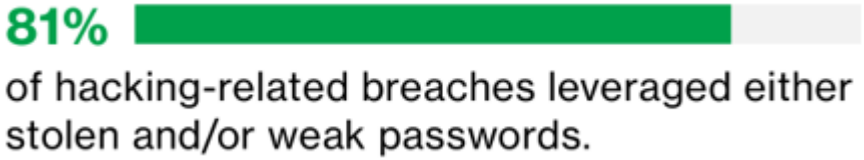
Copyright © 2018 Black Swan Consulting Group Pty Ltd

Think your company is safe?

Positive Technologies: our testers had a 100% success rate at gaining full control over the entire infrastructure in 2016 (as compared to 82% in 2015).

Source: Positive Technologies Security Trends & Vulnerabilities Review, Corporate Information Systems 2017

Source: https://staysmartonlinegreen-site.govcms.gov.au



Source: Verizon Data Breach Investigations Report 2017

Your employees' passwords:

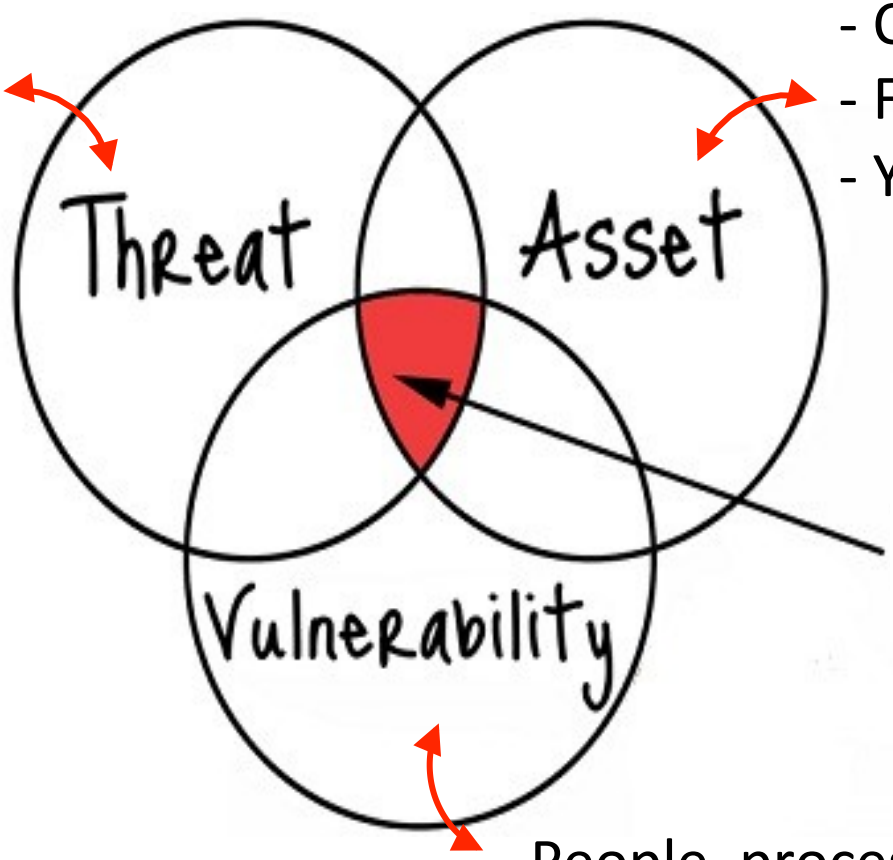
RANK	PASSWORD	CHANGE FROM 2015
1	123456	Unchanged
2	password	Unchanged
3	12345	2 ↗
4	12345678	1 ↘
5	football	2 ↗
6	qwerty	2 ↘
7	1234567890	5 ↗
8	1234567	1 ↗
9	princess	12 ↗
10	1234	2 ↘

Source: https://www.teamsid.com/worst-passwords-2016/?nabe=4561770576609280:1.5716650381017088:0.5767892520140800:2

Copyright © 2018 Black Swan Consulting Group Pty Ltd

Cyber risk

- Cybercriminals
- Their malware



- Customer records
- Finance system
- Your login credentials

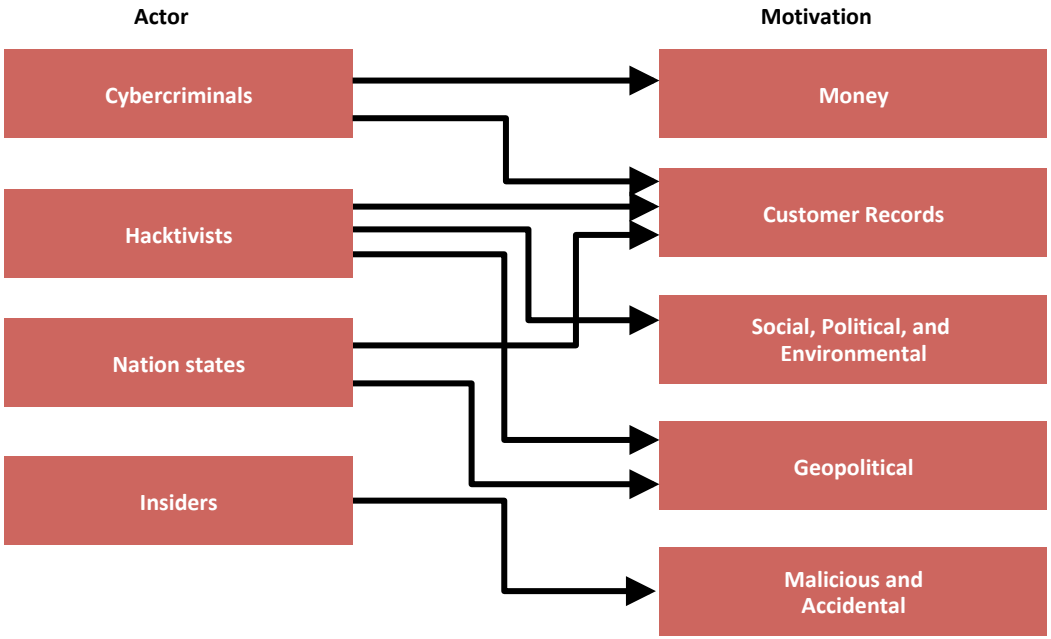
Cyber Risk

- People, process or technology weakness

Image: Google Images

Copyright © 2018 Black Swan Consulting Group Pty Ltd

Cyberattackers & their malware

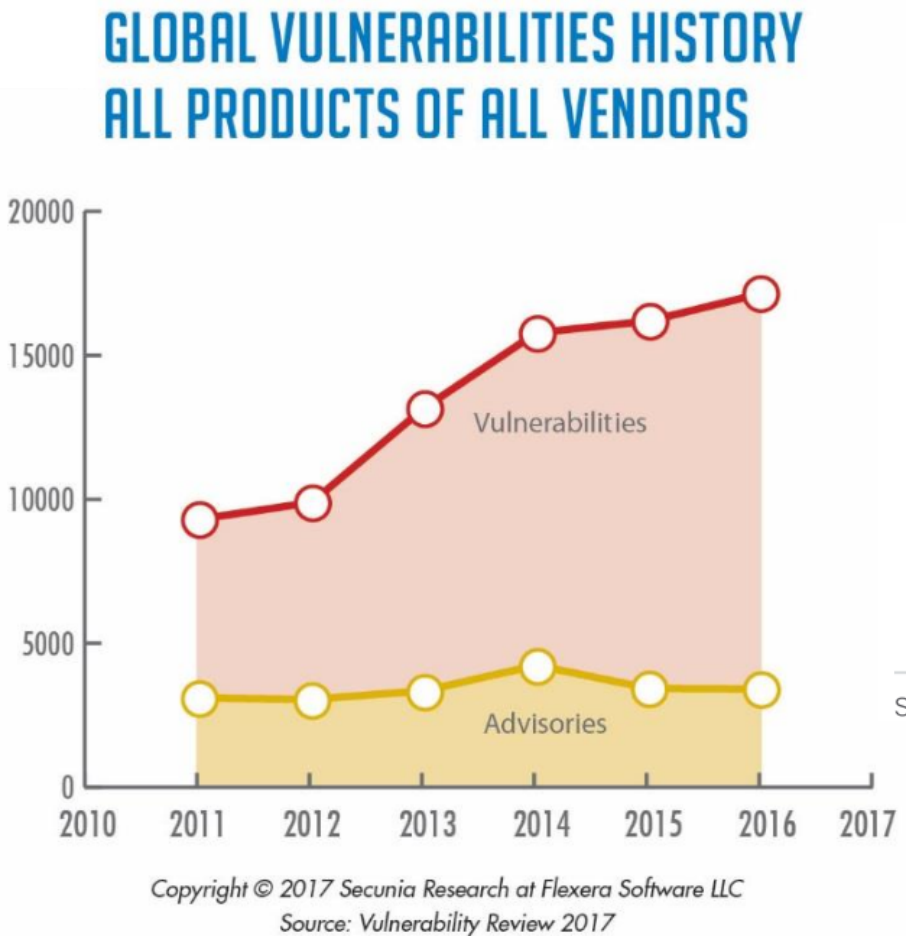


- Viruses
- Ransomware
- Keyloggers
- Root kits
- Trojans
- Backdoors
- Bots

Image: Google Images

Copyright © 2018 Black Swan Consulting Group Pty Ltd

Where we're vulnerable



Server Vulnerabilities
(From 2332 to 3142)
▲34%

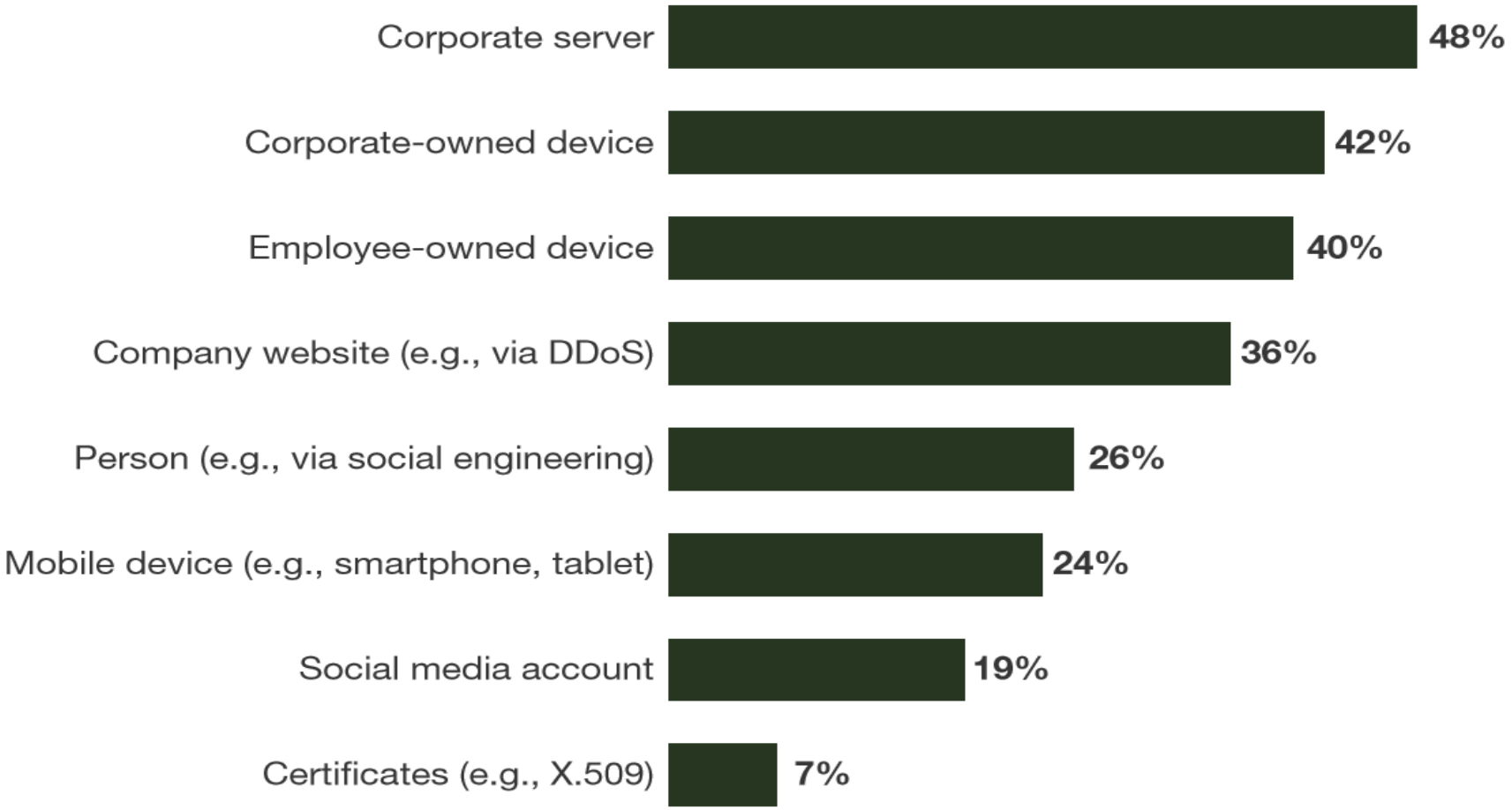
Client Vulnerabilities
(From 2300 to 2106)
▼8%

Network Vulnerabilities
(From 501 to 396)
▼20%

Source: National Vulnerability Database

Copyright © 2018 Black Swan Consulting Group Pty Ltd

Assets under cyberattack



Source: Forrester's Global Business Technographics® Security Survey, 2016

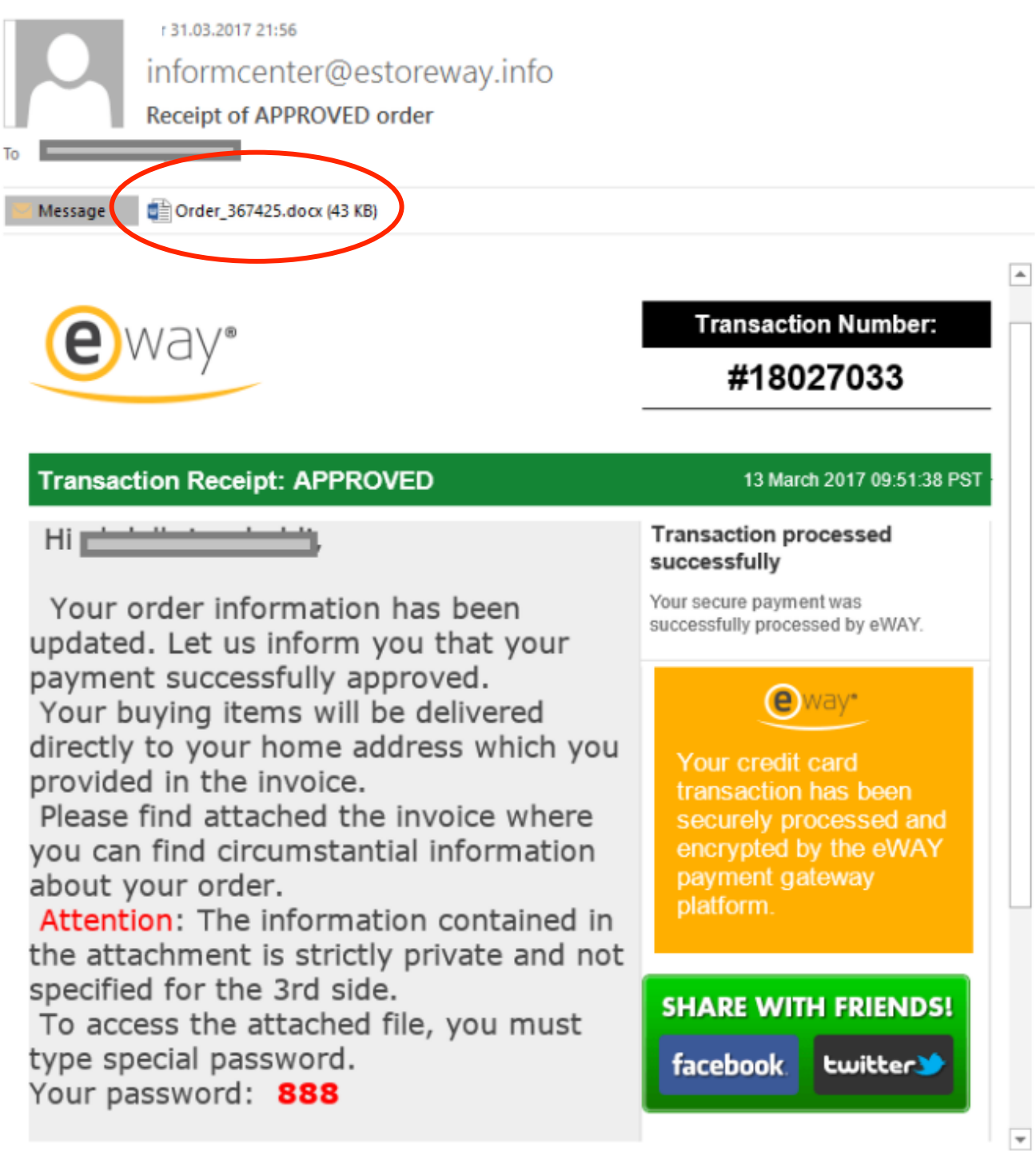
Copyright © 2018 Black Swan Consulting Group Pty Ltd

Phishing

- Just like sports fishing where the cyberattacker uses ‘bait’ to get you to do what s/he wants you to do:
  - Click on a malware infected email attachment
  - Click on a link in an email to a malware infected website
- Phishing was the number one attack vector for 2017 & 2016

Image: Google Images

Copyright © 2018 Black Swan Consulting Group Pty Ltd


r 31.03.2017 21:56

informcenter@estoreway.info

Receipt of APPROVED order

To [redacted]

Message Order_367425.docx (43 KB)

eway®

Transaction Number:

#18027033

Transaction Receipt: APPROVED 13 March 2017 09:51:38 PST

Hi [redacted]

Your order information has been updated. Let us inform you that your payment successfully approved.
Your buying items will be delivered directly to your home address which you provided in the invoice.
Please find attached the invoice where you can find circumstantial information about your order.
Attention: The information contained in the attachment is strictly private and not specified for the 3rd side.
To access the attached file, you must type special password.
Your password: **888**

Transaction processed successfully

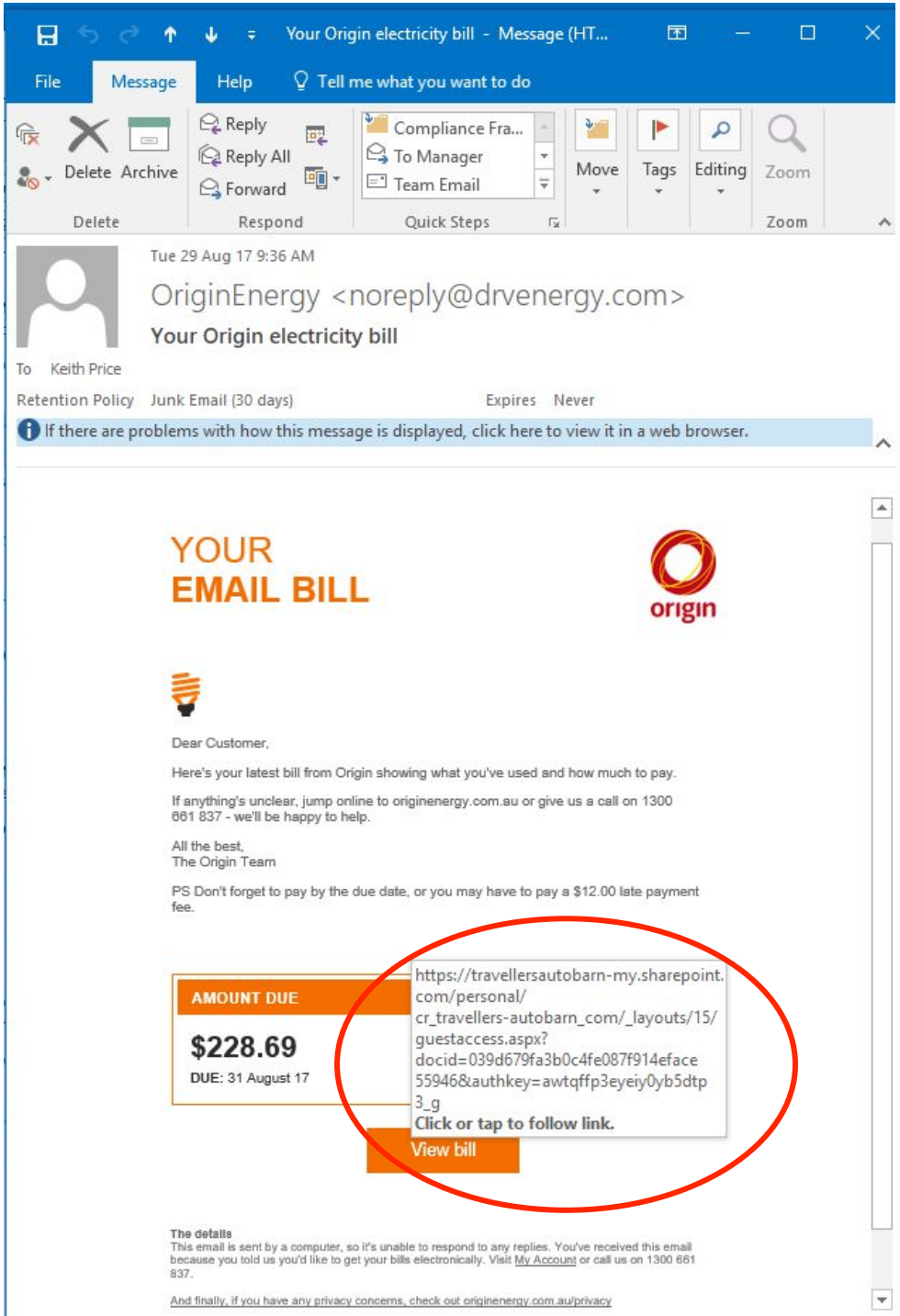
Your secure payment was successfully processed by eWAY.

eway

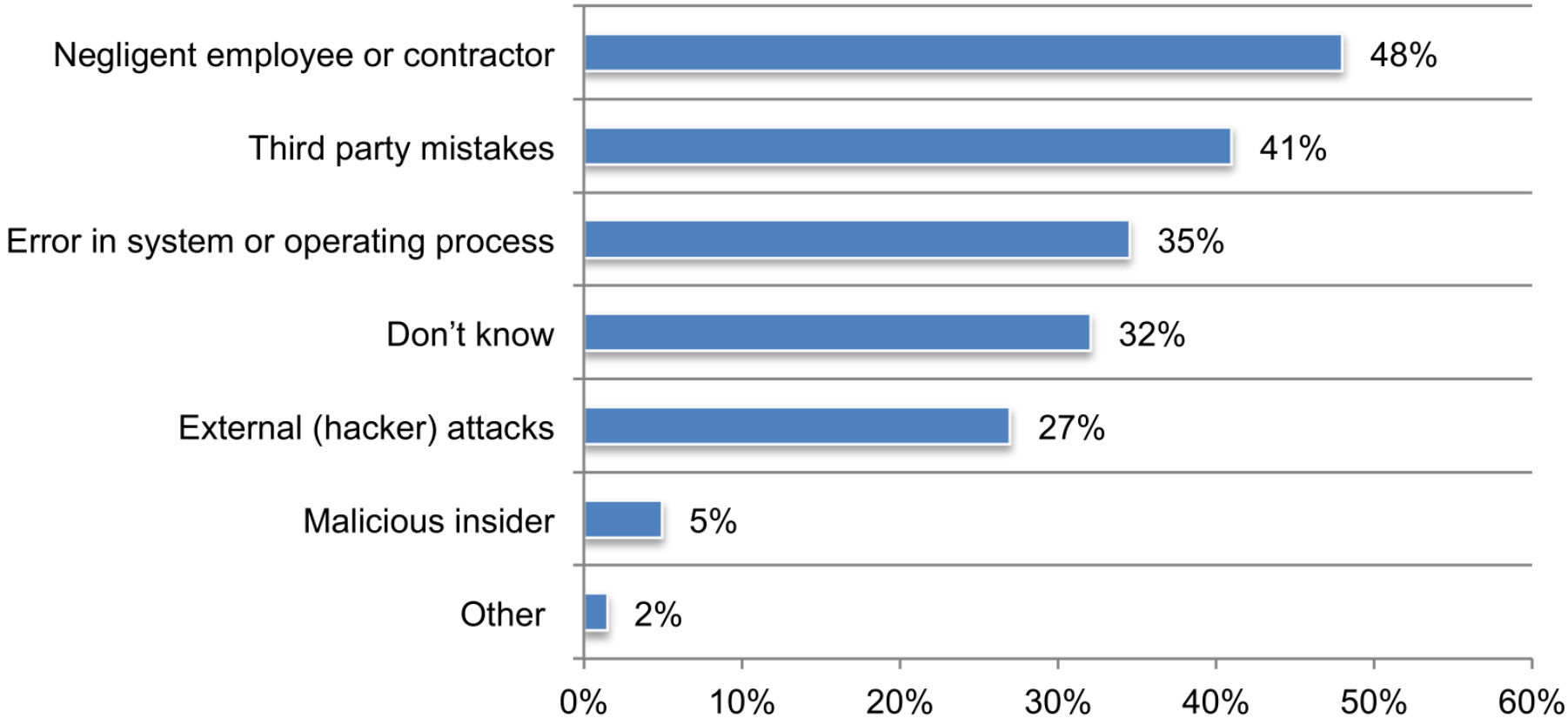
Your credit card transaction has been securely processed and encrypted by the eWAY payment gateway platform.

SHARE WITH FRIENDS!

facebook twitter


Your Origin electricity bill - Message (HT...
File
Message
Help
Tell me what you want to do
Delete
Archive
Reply
Reply All
Forward
Compliance Fra...
To Manager
Team Email
Move
Tags
Editing
Zoom
Delete
Respond
Quick Steps
Zoom
Tue 29 Aug 17 9:36 AM
OriginEnergy <noreply@drvenergy.com>
Your Origin electricity bill
To Keith Price
Retention Policy Junk Email (30 days)
Expires Never
If there are problems with how this message is displayed, click here to view it in a web browser.
YOUR
EMAIL BILL
origin
Dear Customer,
Here's your latest bill from Origin showing what you've used and how much to pay.
If anything's unclear, jump online to originenergy.com.au or give us a call on 1300 661 837 - we'll be happy to help.
All the best,
The Origin Team
PS Don't forget to pay by the due date, or you may have to pay a $12.00 late payment fee.
AMOUNT DUE
$228.69
DUE: 31 August 17
https://travellersautobarn-my.sharepoint.com/personal/cr_travellers-autobarn_com/_layouts/15/guestaccess.aspx?docid=039d679fa3b0c4fe087f914eface55946&authkey=awtqffp3eyeiy0yb5dtp3_g
Click or tap to follow link.
View bill
The details
This email is sent by a computer, so it's unable to respond to any replies. You've received this email because you told us you'd like to get your bills electronically. Visit My Account or call us on 1300 661 837.
And finally, if you have any privacy concerns, check out originenergy.com.au/privacy

Root causes of data breaches



Source: The Forrester Wave™: Endpoint Security Suites, Q4 2016

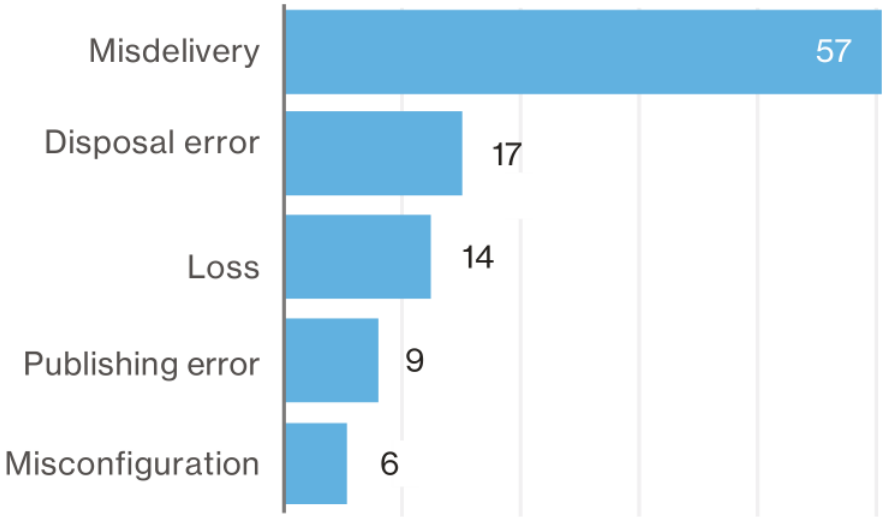
Copyright © 2018 Black Swan Consulting Group Pty Ltd

Insider threat

Privileged users were the top insider threat in all regions save Japan.

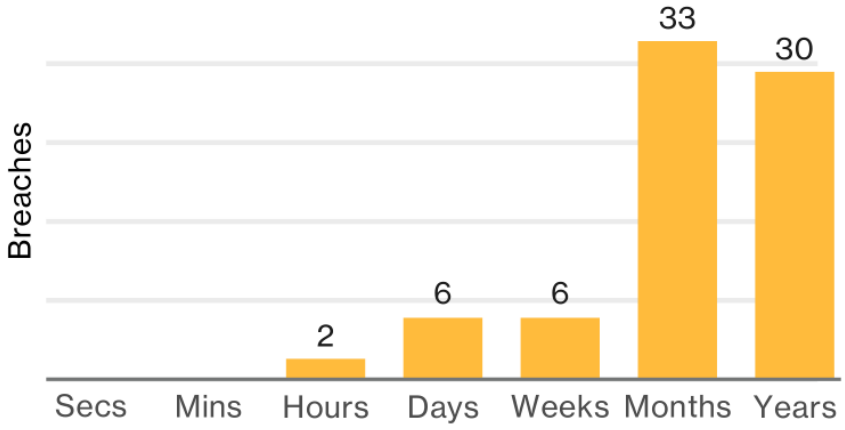
Source: Thales Data Threat Report Global Edition 2017

Cause of insider breaches



Verizon Data Breach Investigations Report 2017

Breach discovery timeline of insider breaches



Verizon Data Breach Investigations Report 2017

Copyright © 2018 Black Swan Consulting Group Pty Ltd

National Institute of Standards and Technology
U.S. Department of Commerce

black swan group

- Framework for Improving Critical Infrastructure Cybersecurity

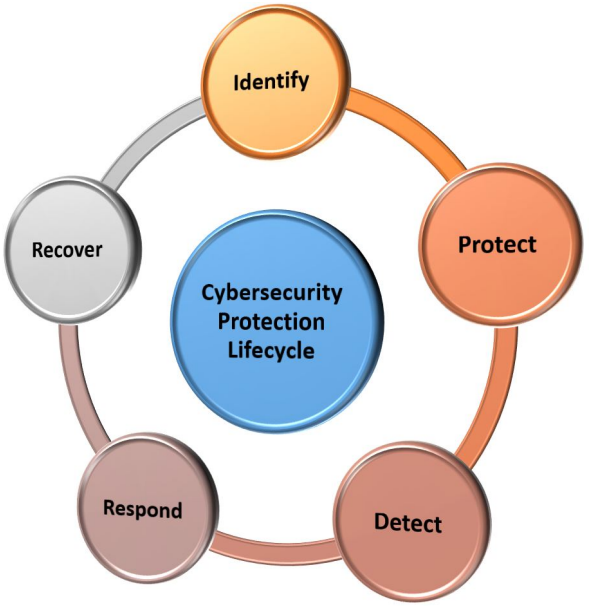
- "The Framework enables organisations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure."

Copyright © 2018 Black Swan Consulting Group Pty Ltd

Cybersecurity protection lifecycle

Five functions:

1. Identifying data, systems, services, and risk strategy
2. Protecting information and systems to ensure delivery of mission critical services.
3. Detecting a cybersecurity event
4. Responding to a cybersecurity event
5. Maintaining resilience and recovering quickly to restore the services



Source: US NIST Cybersecurity Framework, www.nist.gov

Copyright © 2018 Black Swan Consulting Group Pty Ltd

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Source: US NIST

Advice

- Accept that your organisation is a target.
  - *Because every organisation is a target.*
- Accept that there are no trivial systems in your network.
  - *Attackers will exploit any opening to break in, then move laterally compromising other systems & applications.*
- Accept that it's not possible to protect everything.
  - *Identify & protect your most critical information and systems.*
- Accept that cyberattackers & malware are going to get in.
  - *Advise your management to focus resources on detecting and responding to attacks as early as possible to minimise the damage.*

Copyright © 2018 Black Swan Consulting Group Pty Ltd

Advice

- Use a cybersecurity assessment to inform which controls are needed to provide the greatest cyber risk reduction.

- Protect the rest of your network from compromised desktops, laptops, and Internet-facing web services by segmenting the network.

- Offense informs defence:
  - *Use knowledge of actual attacks to continually improve your cyber defences.*

Key takeaway: cybersecurity is not an IT problem.

Copyright © 2018 Black Swan Consulting Group Pty Ltd