LonMark International

Cybersecurity & IT Integration for Commercial Buildings

"*While traditional information systems generally prioritize Confidentiality, then Integrity, and lastly Availability, control systems and IoT usually prioritize Availability first, then Integrity and lastly Confidentiality.“*

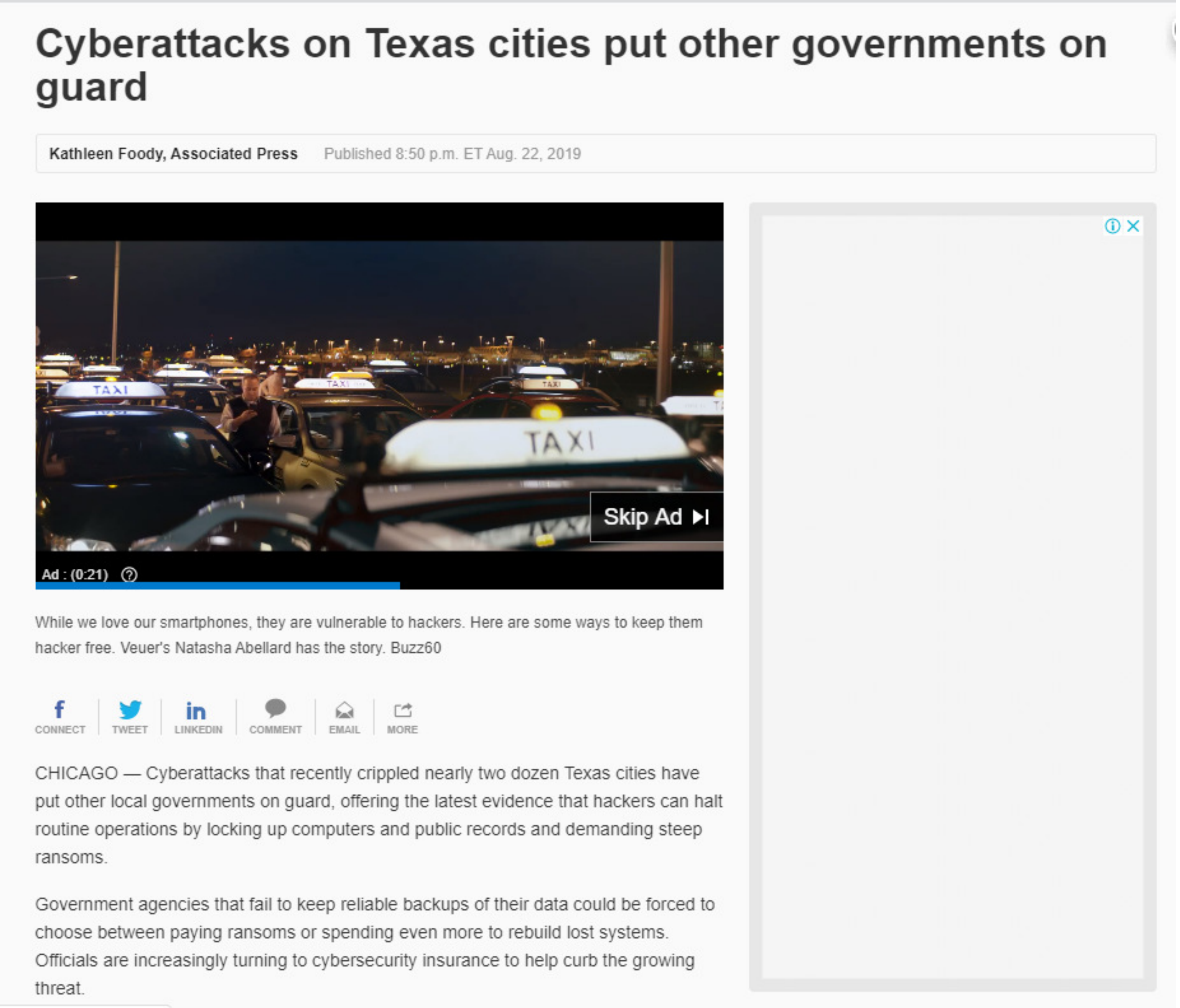
Draft NISTIR 8200 Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)

"...there is a small - and rapidly closing - window to ensure that IoT is adopted in a way that maximizes security and minimizes risk. If the country fails to do so, it will be coping with the consequences for generations.“

US National Security Telecommunications Advisory Committee, ("NSTAC")

Notable Cybersecurity Breaches

Texas Cyber Attacks, August 2019



Cyberattacks on Texas cities put other governments on guard

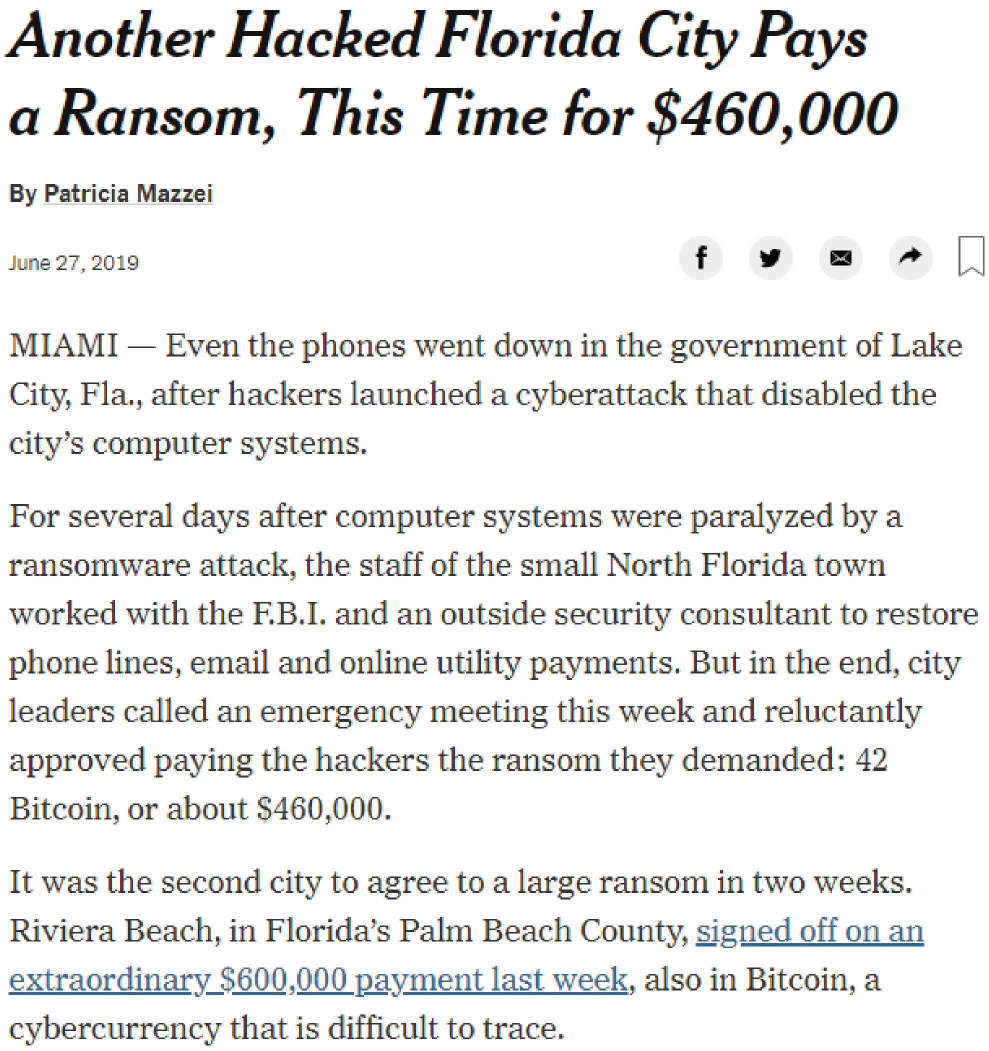
Kathleen Foody, Associated Press Published 8:50 p.m. ET Aug. 22, 2019

While we love our smartphones, they are vulnerable to hackers. Here are some ways to keep them hacker free. Veuer's Natasha Abellard has the story. Buzz60

CHICAGO — Cyberattacks that recently crippled nearly two dozen Texas cities have put other local governments on guard, offering the latest evidence that hackers can halt routine operations by locking up computers and public records and demanding steep ransoms.

Government agencies that fail to keep reliable backups of their data could be forced to choose between paying ransoms or spending even more to rebuild lost systems. Officials are increasingly turning to cybersecurity insurance to help curb the growing threat.

Lake City Cyber Attack, June 2019



Another Hacked Florida City Pays a Ransom, This Time for $460,000

By Patricia Mazzei

June 27, 2019

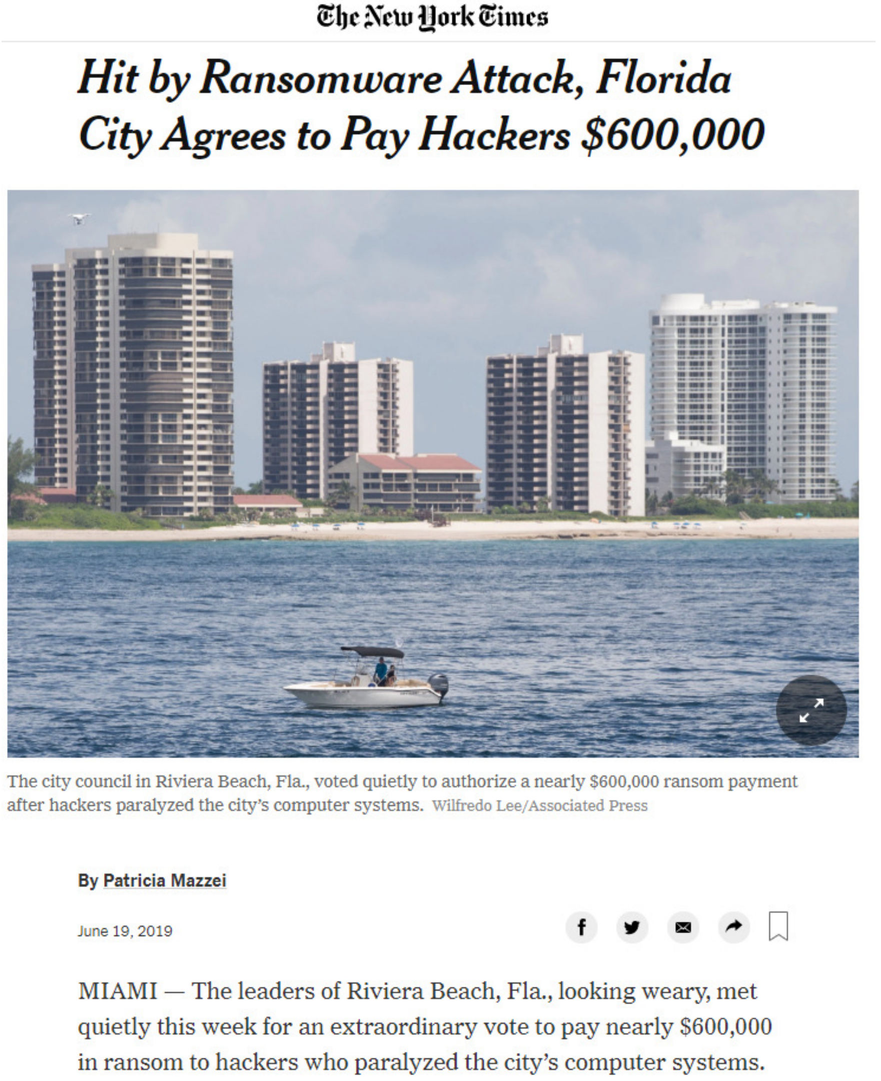
MIAMI — Even the phones went down in the government of Lake City, Fla., after hackers launched a cyberattack that disabled the city's computer systems.

For several days after computer systems were paralyzed by a ransomware attack, the staff of the small North Florida town worked with the F.B.I. and an outside security consultant to restore phone lines, email and online utility payments. But in the end, city leaders called an emergency meeting this week and reluctantly approved paying the hackers the ransom they demanded: 42 Bitcoin, or about $460,000.

It was the second city to agree to a large ransom in two weeks. Riviera Beach, in Florida's Palm Beach County, signed off on an extraordinary $600,000 payment last week, also in Bitcoin, a cybercurrency that is difficult to trace.

LONMARK

Riviera Beach Cyber Attack, June 2019



The New York Times

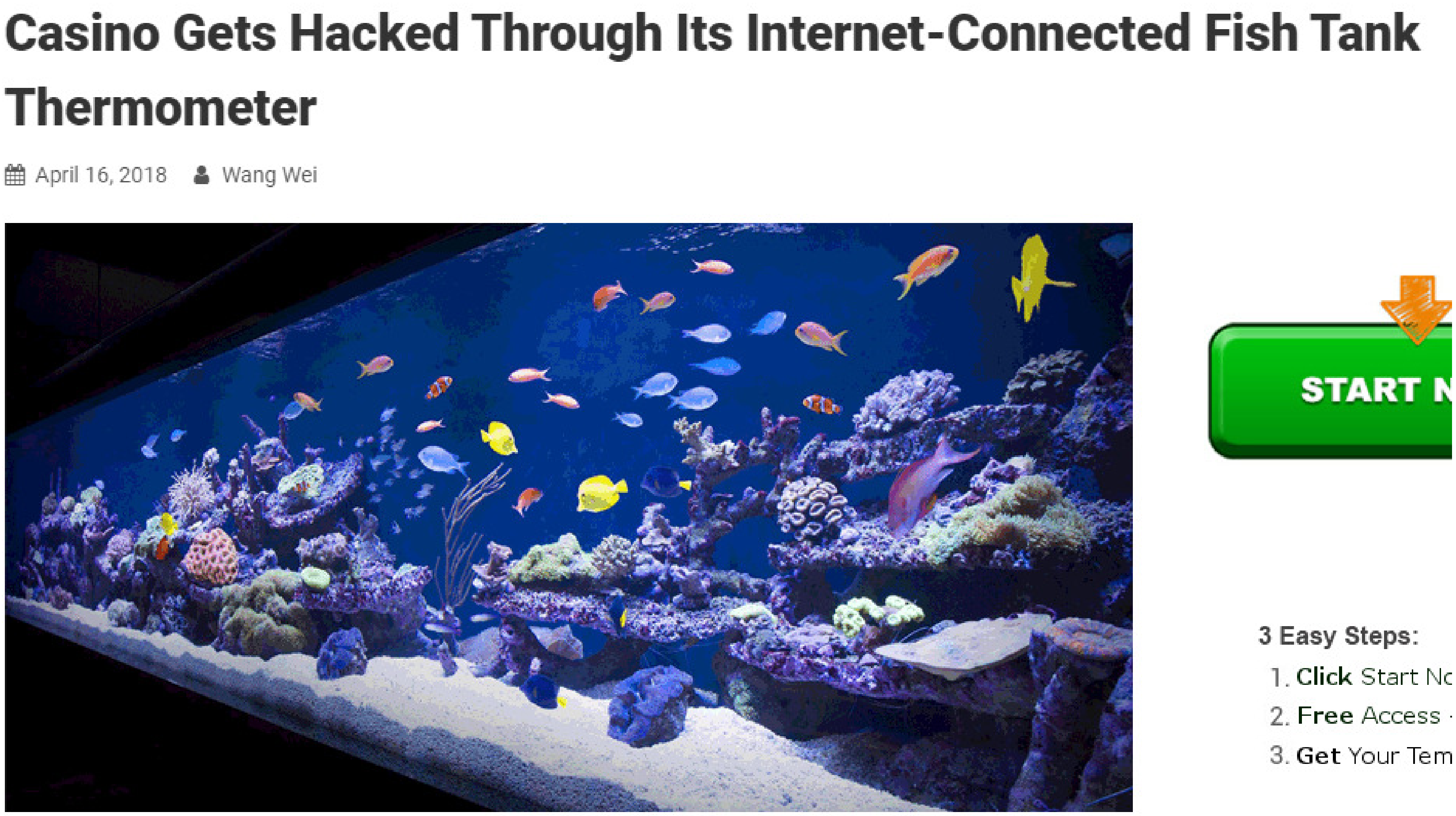
Hit by Ransomware Attack, Florida City Agrees to Pay Hackers $600,000

The city council in Riviera Beach, Fla., voted quietly to authorize a nearly $600,000 ransom payment after hackers paralyzed the city's computer systems. Wilfredo Lee/Associated Press

By Patricia Mazzei

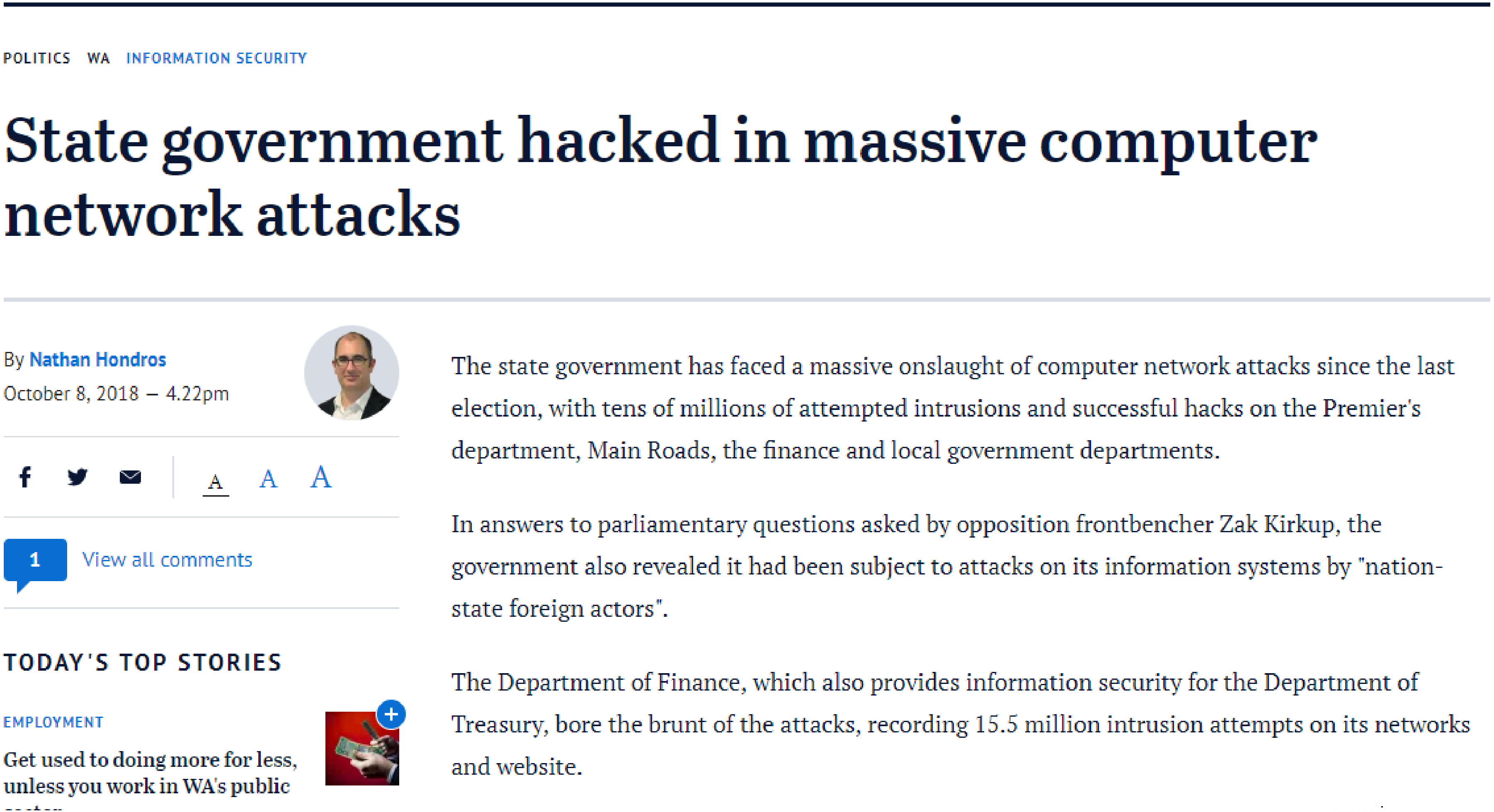
June 19, 2019

MIAMI — The leaders of Riviera Beach, Fla., looking weary, met quietly this week for an extraordinary vote to pay nearly $600,000 in ransom to hackers who paralyzed the city's computer systems.



Casino Gets Hacked Through Its Internet-Connected Fish Tank Thermometer

April 16, 2018 Wang Wei



POLITICS WA INFORMATION SECURITY

State government hacked in massive computer network attacks

By Nathan Hondros
October 8, 2018 – 4.22pm

The state government has faced a massive onslaught of computer network attacks since the last election, with tens of millions of attempted intrusions and successful hacks on the Premier's department, Main Roads, the finance and local government departments.

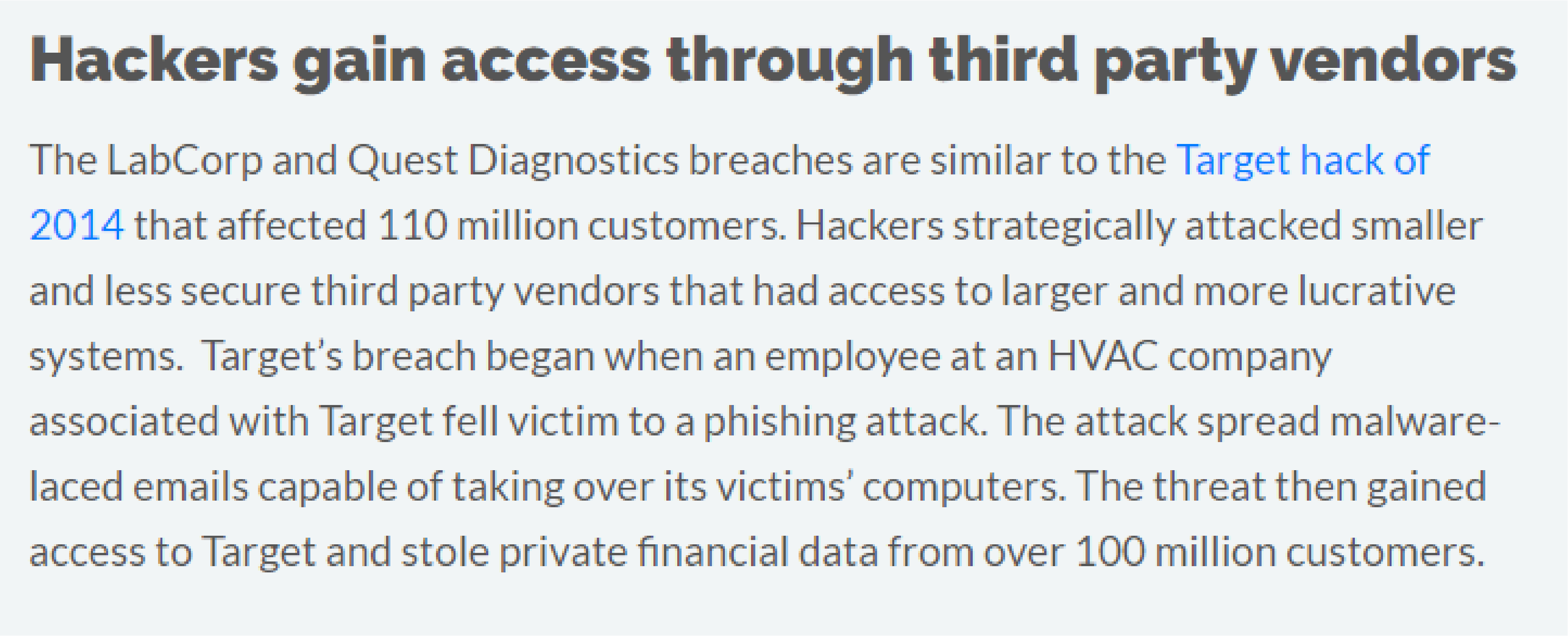
In answers to parliamentary questions asked by opposition frontbencher Zak Kirkup, the government also revealed it had been subject to attacks on its information systems by "nation-state foreign actors".

The Department of Finance, which also provides information security for the Department of Treasury, bore the brunt of the attacks, recording 15.5 million intrusion attempts on its networks and website.

TODAY'S TOP STORIES

EMPLOYMENT

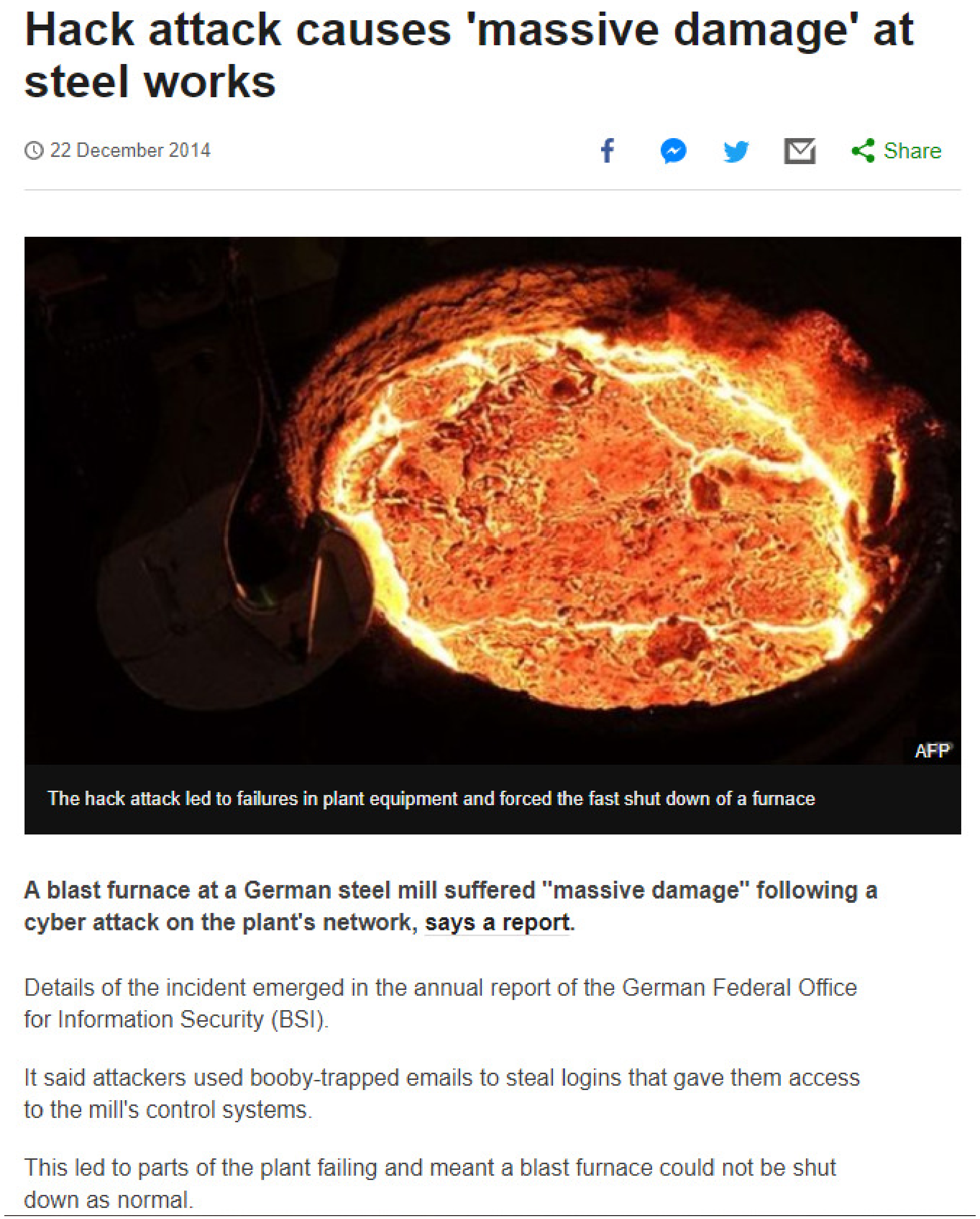
Get used to doing more for less, unless you work in WA's public



Hackers gain access through third party vendors

The LabCorp and Quest Diagnostics breaches are similar to the Target hack of 2014 that affected 110 million customers. Hackers strategically attacked smaller and less secure third party vendors that had access to larger and more lucrative systems. Target’s breach began when an employee at an HVAC company associated with Target fell victim to a phishing attack. The attack spread malware-laced emails capable of taking over its victims’ computers. The threat then gained access to Target and stole private financial data from over 100 million customers.

Fines, Penalties & Costs



Hack attack causes 'massive damage' at steel works

22 December 2014

The hack attack led to failures in plant equipment and forced the fast shut down of a furnace

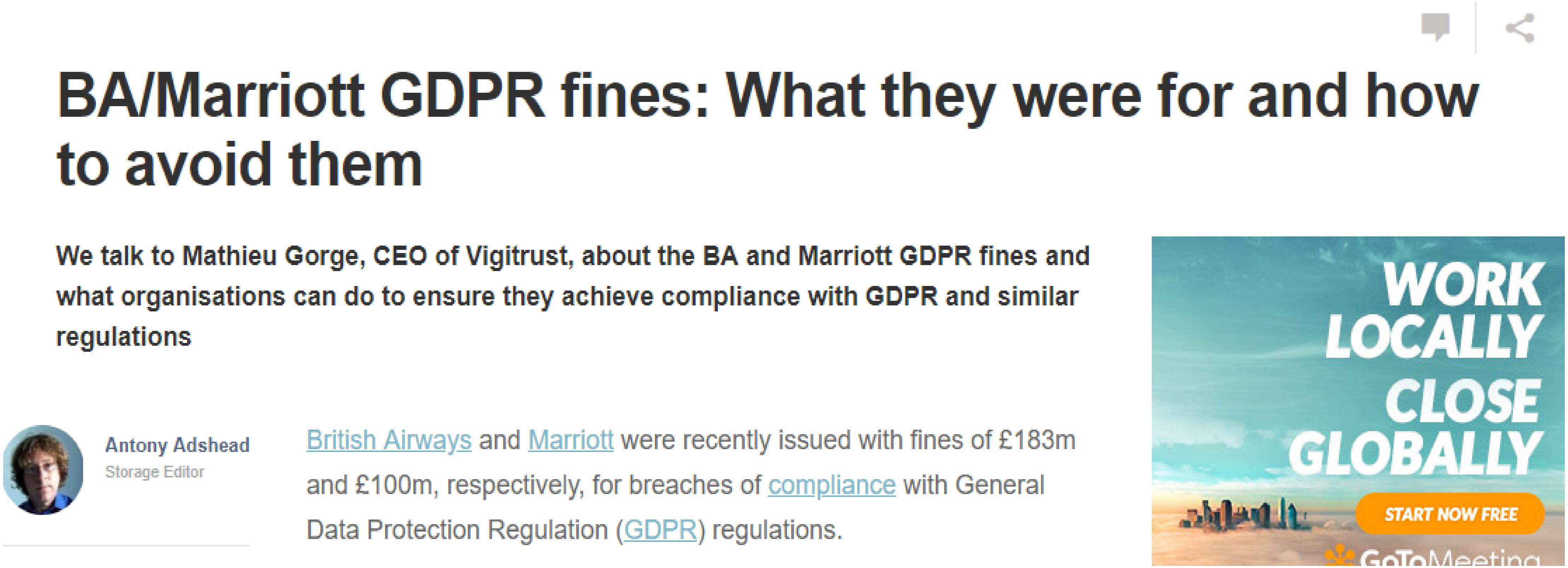
A blast furnace at a German steel mill suffered "massive damage" following a cyber attack on the plant's network, says a report.

Details of the incident emerged in the annual report of the German Federal Office for Information Security (BSI).

It said attackers used booby-trapped emails to steal logins that gave them access to the mill's control systems.

This led to parts of the plant failing and meant a blast furnace could not be shut down as normal.

British Airways & Marriott GDPR Fines



BA/Marriott GDPR fines: What they were for and how to avoid them

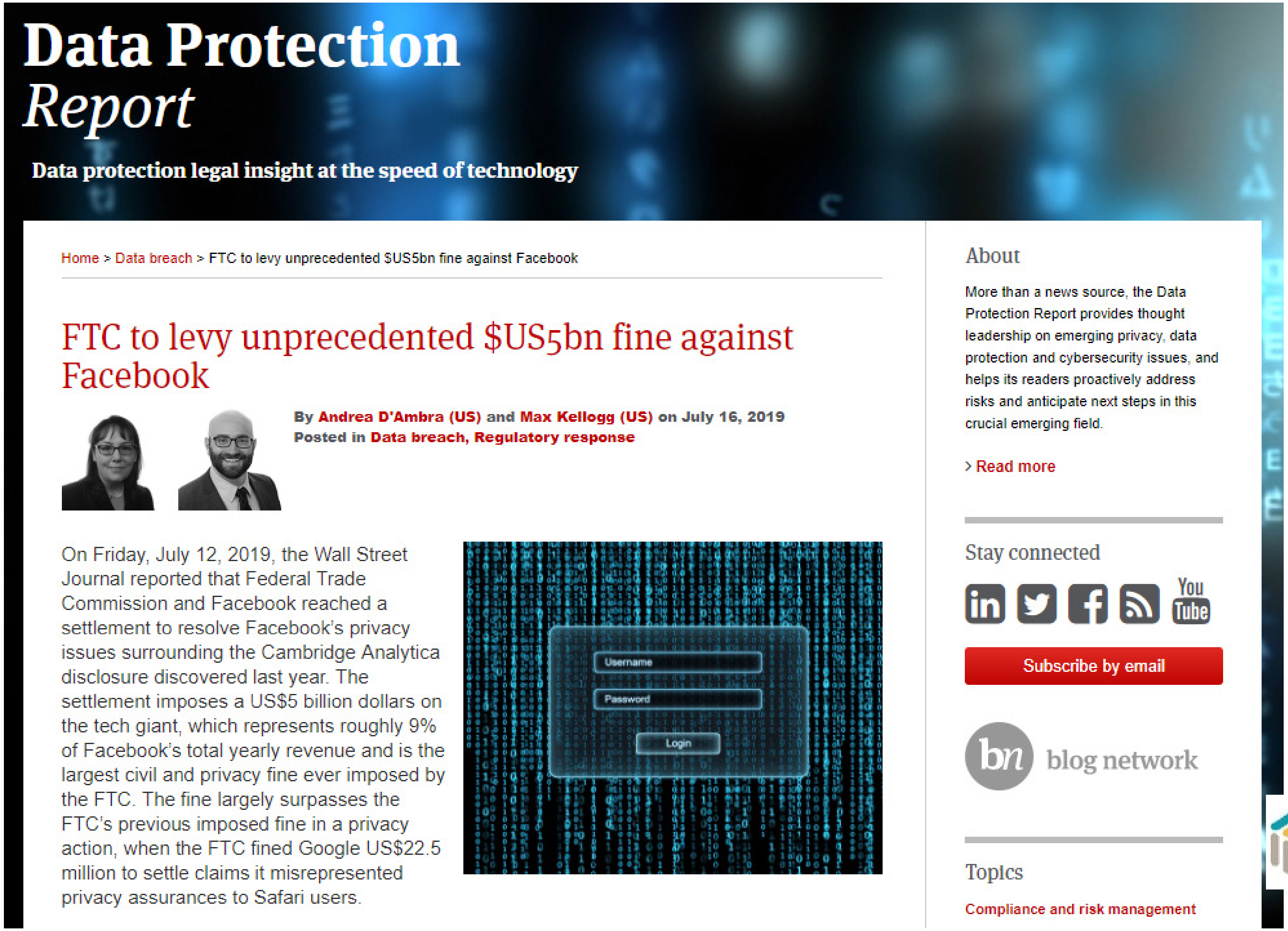
We talk to Mathieu Gorge, CEO of Vigitrust, about the BA and Marriott GDPR fines and what organisations can do to ensure they achieve compliance with GDPR and similar regulations

Antony Adshead
Storage Editor

British Airways and Marriott were recently issued with fines of £183m and £100m, respectively, for breaches of compliance with General Data Protection Regulation (GDPR) regulations.

LONMARK

Facebook FTC Fine



Data Protection *Report*

Data protection legal insight at the speed of technology

Home > Data breach > FTC to levy unprecedented $US5bn fine against Facebook

FTC to levy unprecedented $US5bn fine against Facebook

By Andrea D'Ambra (US) and Max Kellogg (US) on July 16, 2019
Posted in Data breach, Regulatory response

On Friday, July 12, 2019, the Wall Street Journal reported that Federal Trade Commission and Facebook reached a settlement to resolve Facebook's privacy issues surrounding the Cambridge Analytica disclosure discovered last year. The settlement imposes a US$5 billion dollars on the tech giant, which represents roughly 9% of Facebook's total yearly revenue and is the largest civil and privacy fine ever imposed by the FTC. The fine largely surpasses the FTC's previous imposed fine in a privacy action, when the FTC fined Google US$22.5 million to settle claims it misrepresented privacy assurances to Safari users.

About

More than a news source, the Data Protection Report provides thought leadership on emerging privacy, data protection and cybersecurity issues, and helps its readers proactively address risks and anticipate next steps in this crucial emerging field.

> Read more

Stay connected

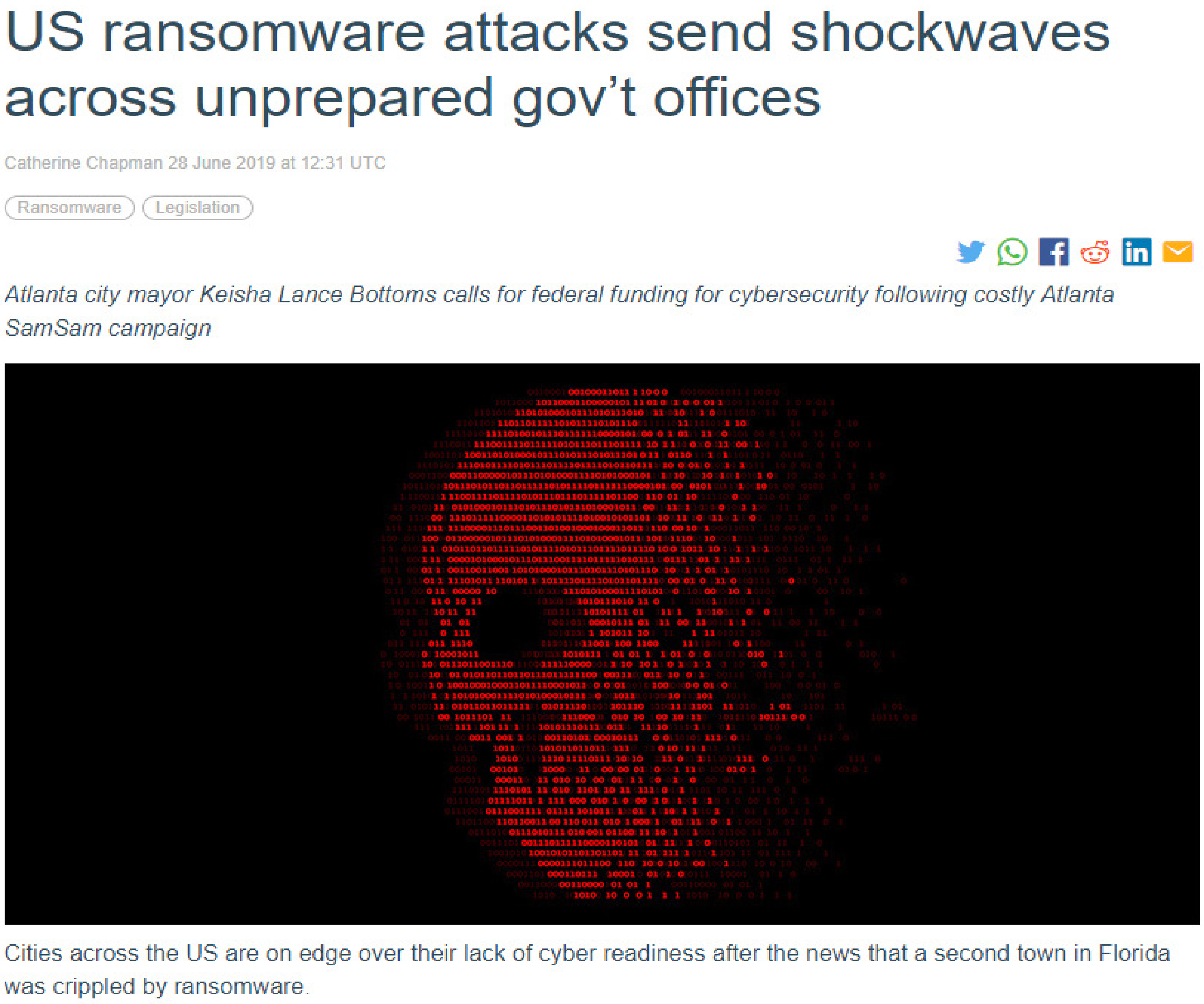
Subscribe by email

bn blog network

Topics

Compliance and risk management

Atlanta, Georgia Cyber Attack, March 2018



US ransomware attacks send shockwaves across unprepared gov't offices

Catherine Chapman 28 June 2019 at 12:31 UTC

Ransomware Legislation

Atlanta city mayor Keisha Lance Bottoms calls for federal funding for cybersecurity following costly Atlanta SamSam campaign

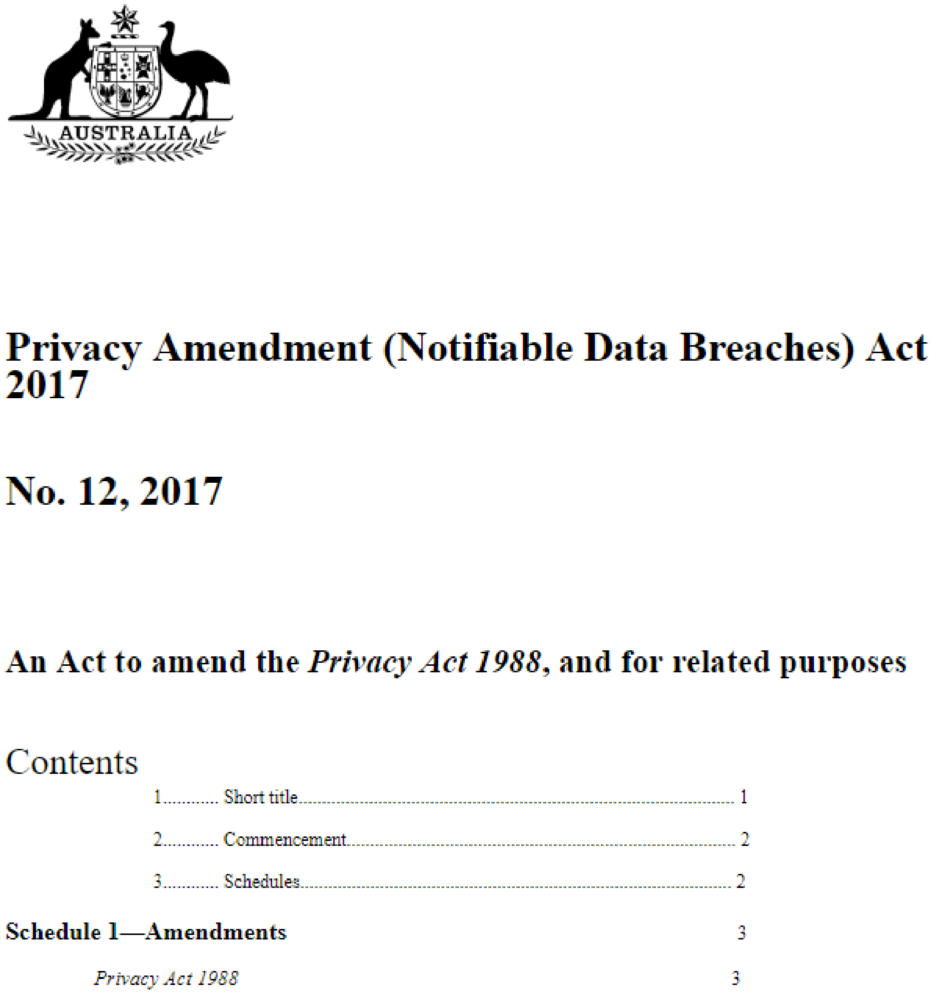
Cities across the US are on edge over their lack of cyber readiness after the news that a second town in Florida was crippled by ransomware.

Atlanta, Georgia Cyber Attack, March 2018

- In January 2018 an audit warned that the city’s IT department lacked some basic security features and there was no adequate plan for dealing with an attack
- 22nd March 2018 the SamSam Ransomware attack took place via Brute Force Attack
- US$9.5m in recovery costs
- US$9.5m in additional ongoing annual cybersecurity costs
- Unquantified operational costs
- 1/3 of 424 software programs offline, (30% “mission critical”)
- City Attorney’s office lost 71 of 77 computers with 10 years’ of records
- 16 years’ of municipal records lost forever
- Police dashcam video lost never to be recovered

Legislation & Regulations

Australian Legislation
Notifiable Data Breaches, (“NDB”)



AUSTRALIA

Privacy Amendment (Notifiable Data Breaches) Act 2017

No. 12, 2017

An Act to amend the *Privacy Act 1988*, and for related purposes

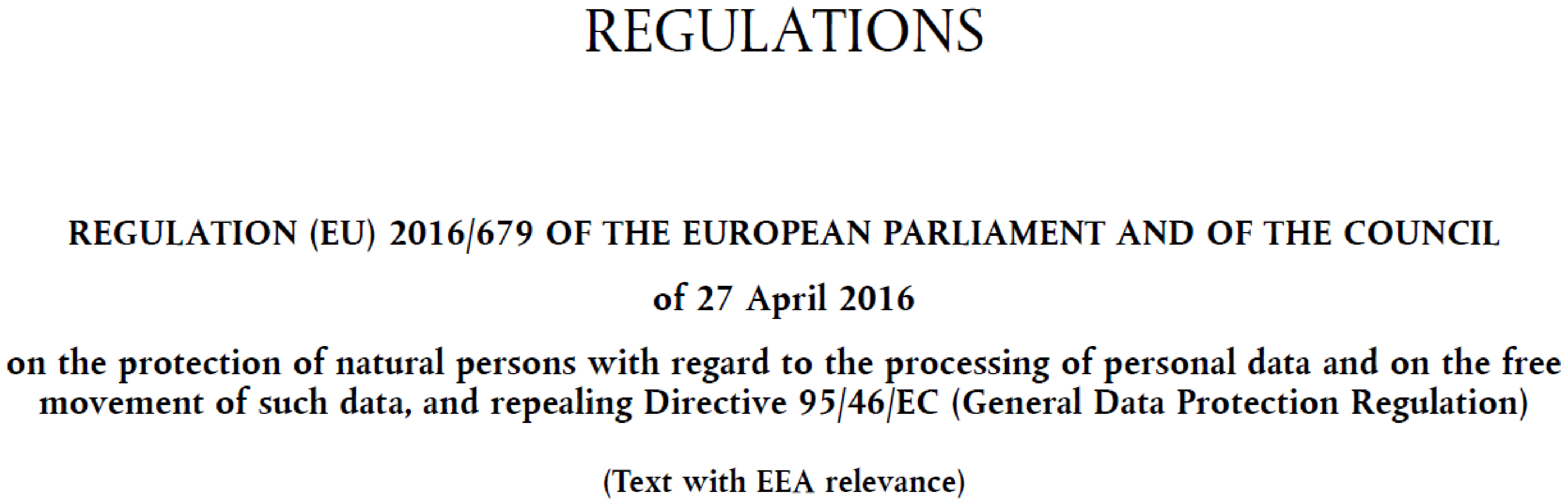
Contents

NDB Penalties – Australia

Since 22nd February 2018, organisations with a turnover of $3million or more fall within the scope of the new Privacy Act measures requiring mandatory notification of cybersecurity breaches.

Penalties for breaches are currently $1.7 million for organisations with revenue of over AUD$3 million annually, and AUD$340,000 for individuals.

General Data Protection Regulations, (“GDPR”)



REGULATIONS

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 27 April 2016

on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

(Text with EEA relevance)

GDPR Breach Penalties

Data controllers and processors face administrative fines of:

•Up to **€10 million or 2% of annual global turnover** for infringements of articles:

- 8 (conditions for children’s consent);
- 11 (processing that doesn’t require identification);
- 25–39 (general obligations of processors and controllers);
- 42 (certification); and
- 43 (certification bodies).

•Up to **€20 million or 4% of annual global turnover** for infringements of articles:

- 5 (data processing principles);
- 6 (lawful bases for processing);
- 7 (conditions for consent);
- 9 (processing of special categories of data);
- 12–22 (data subjects’ rights); and
- 44–49 (data transfers to third countries).

GDPR – Extra-territorial Effect

It is crucial for organisations outside of the EU that may from time to time engage in sharing of data realise that the GDPR is to protect data belonging to EU citizens and residents. The law, therefore, applies to organisations that handle such data whether they are EU-based organisations or not. This legal mechanism is known as "extra-territorial effect."

US FTC Privacy & Data Security

Privacy &
Data Security

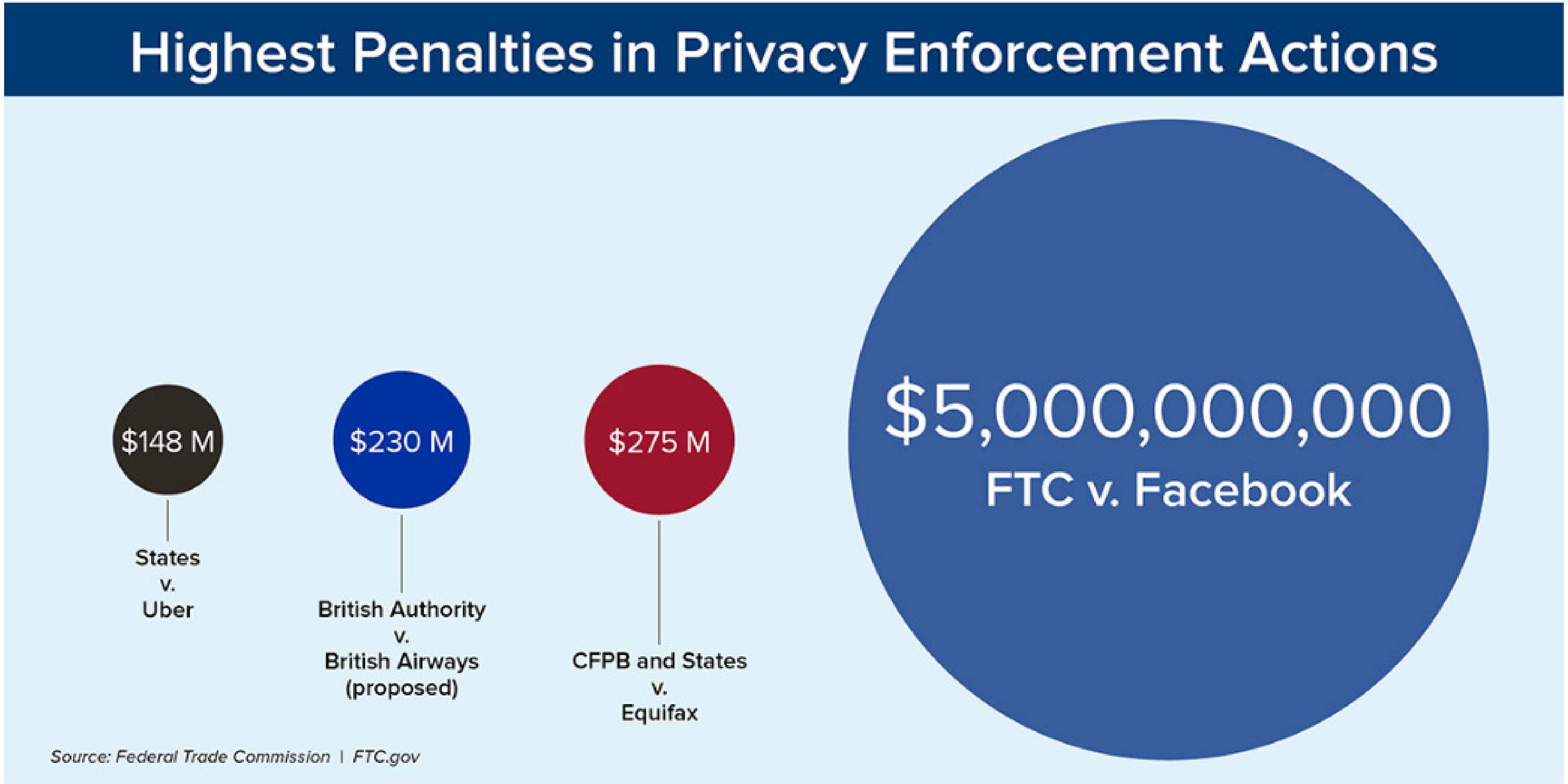
Update: 2018

Federal Trade Commission
January 2018 - December 2018

FEDERAL TRADE COMMISSION ★ UNITED STATES OF AMERICA ★ MCMXV ★

LONMARK®

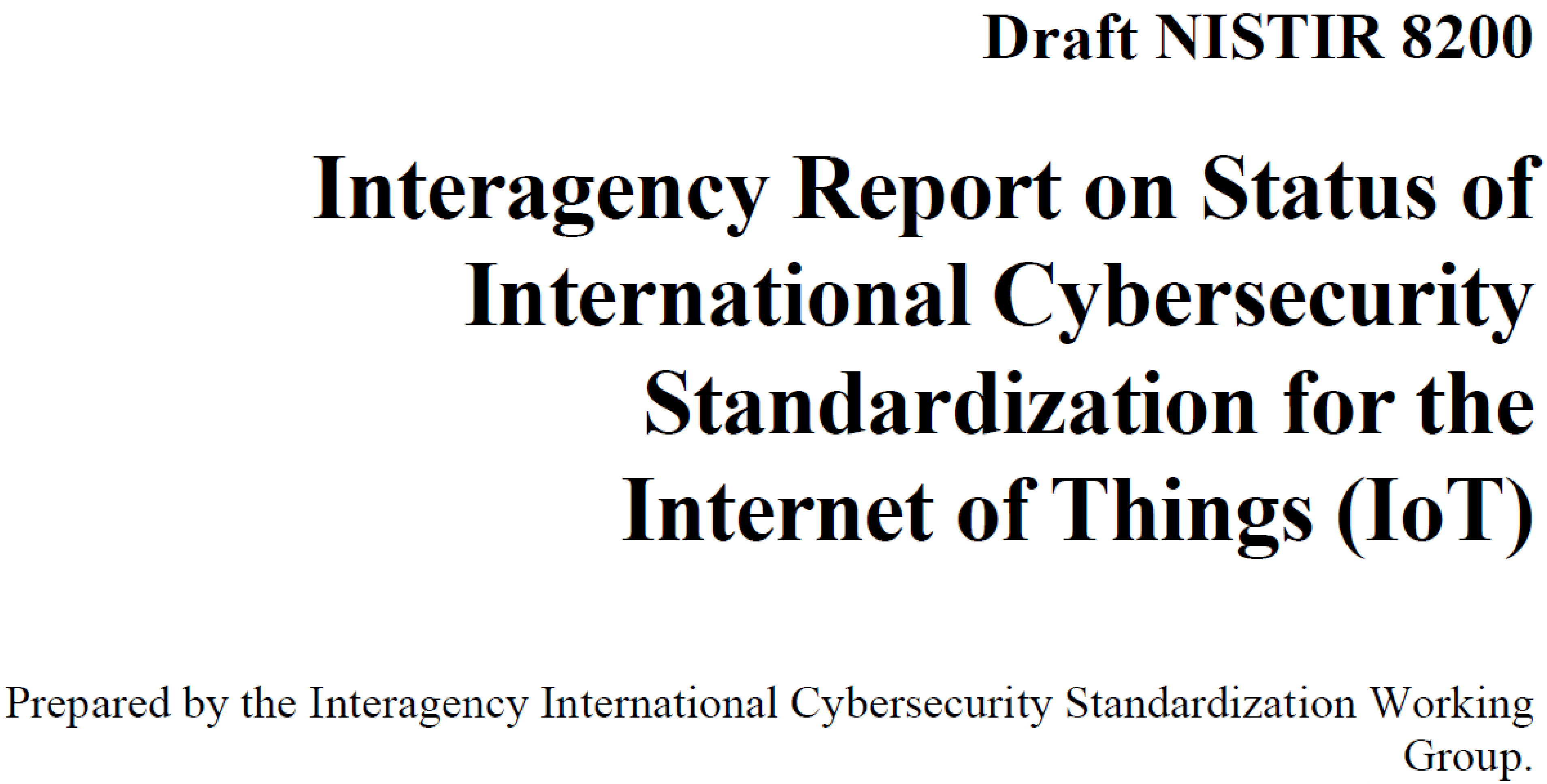
US FTC Privacy & Data Security Penalties



Source: Federal Trade Commission | FTC.gov

The FTC administers a wide variety of laws and regulations, including the Federal Trade Commission Act, Telemarketing Sale Rule, Identity Theft Act, Fair Credit Reporting Act, and Clayton Act. In total, the Commission has enforcement or administrative responsibilities under more than 70 laws.

Reference Documents



Draft NISTIR 8200

Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)

Prepared by the Interagency International Cybersecurity Standardization Working Group.

Australian Government

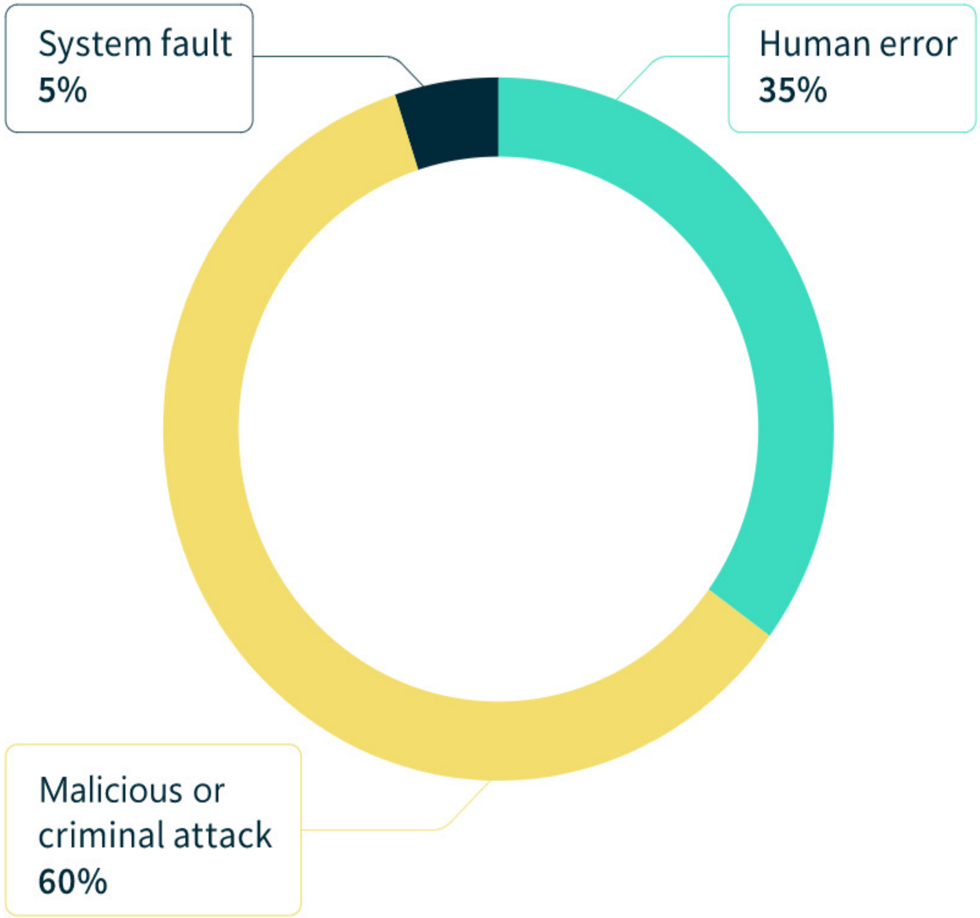
Office of the Australian
Information Commissioner

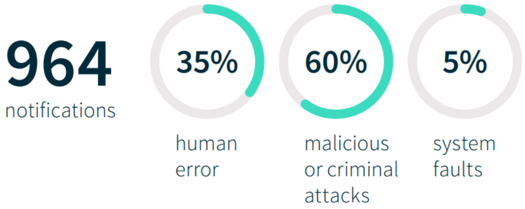
Notifiable Data Breaches Scheme 12-month Insights Report

LONMARK®

Sources of Data Breaches

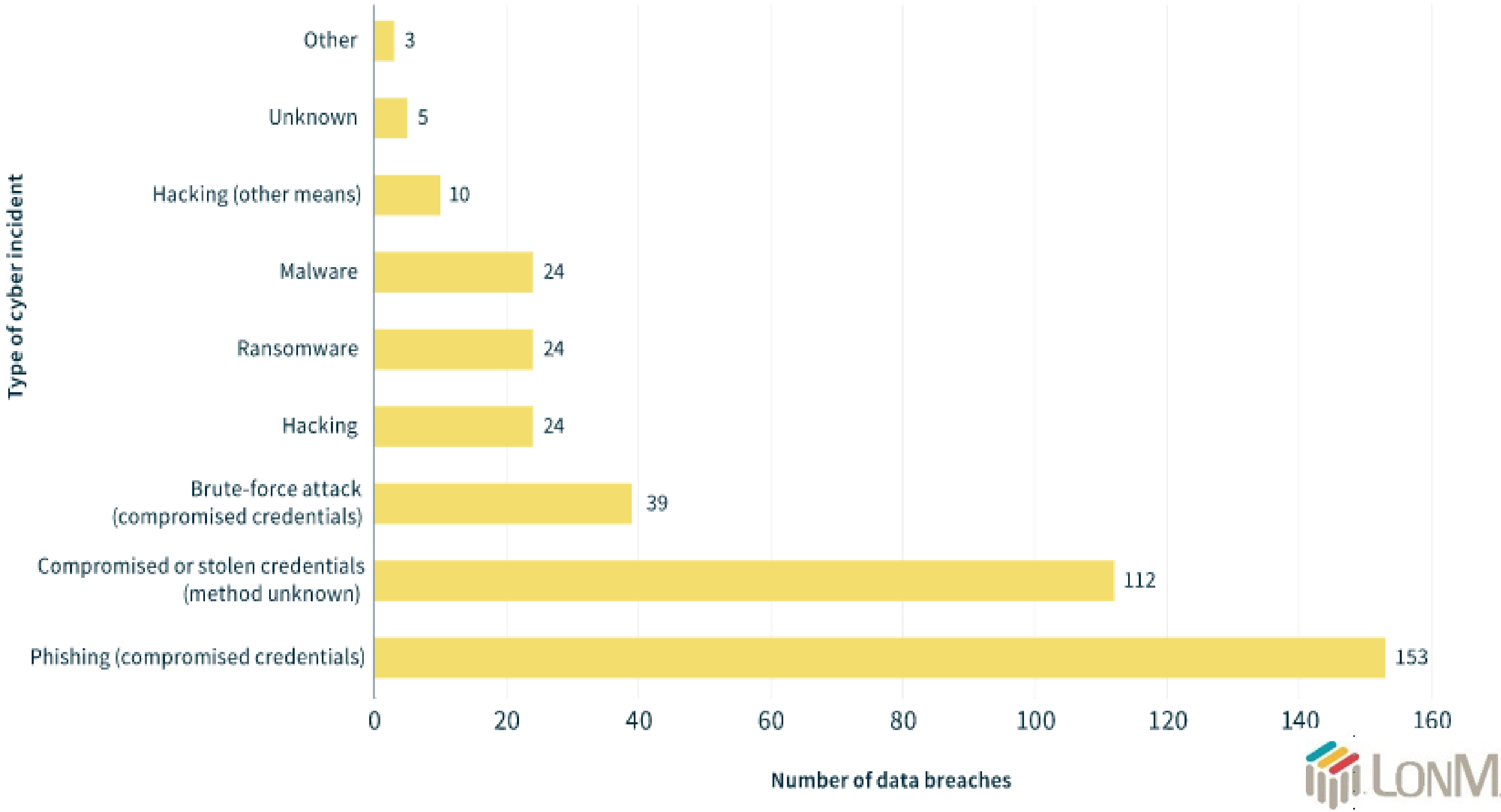
All Sectors from 1 April 2018 to 31 March 2019





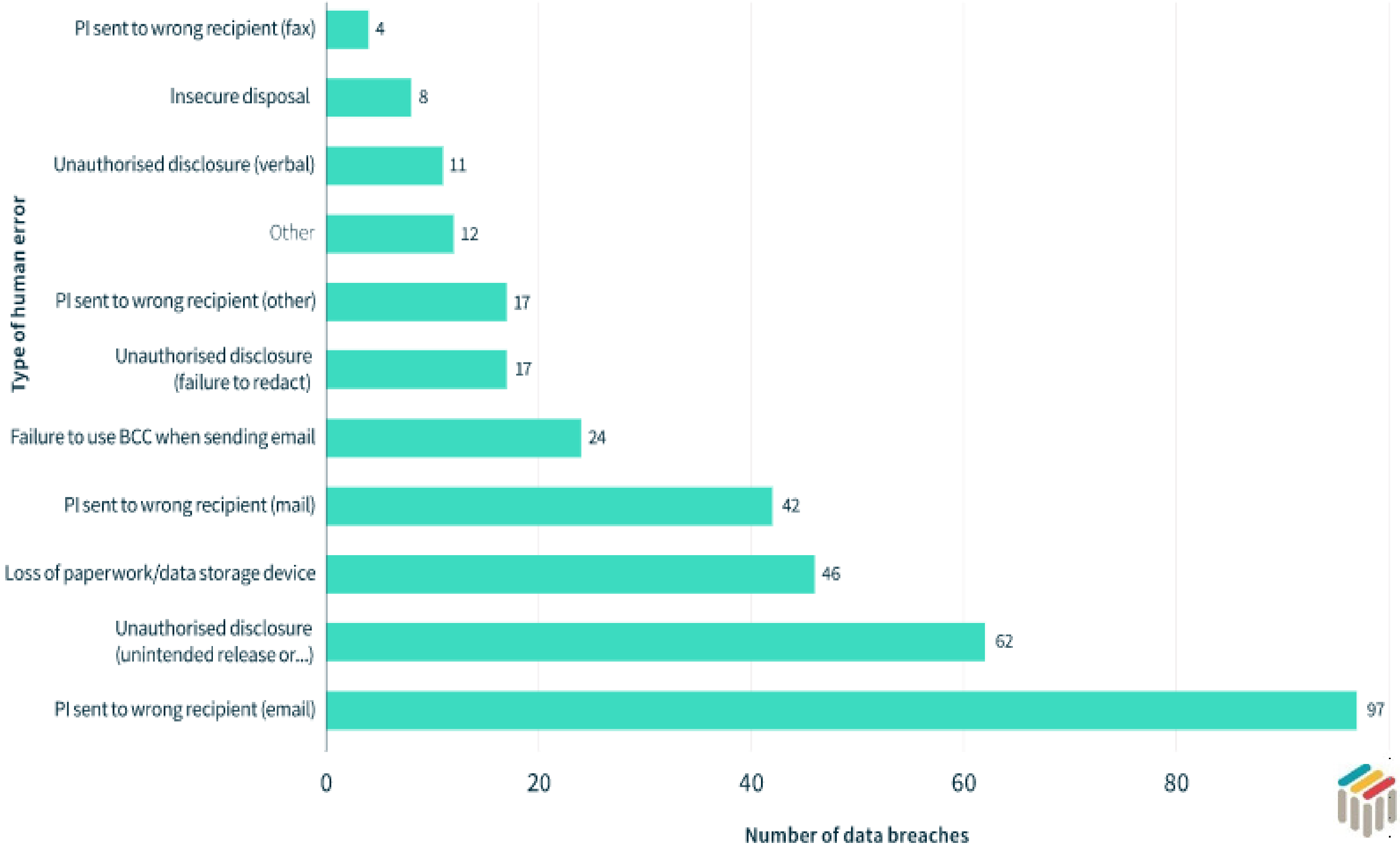
Cyber Incident Breaches

All Sectors from 1 April 2018 to 31 March 2019



Human Error Breaches

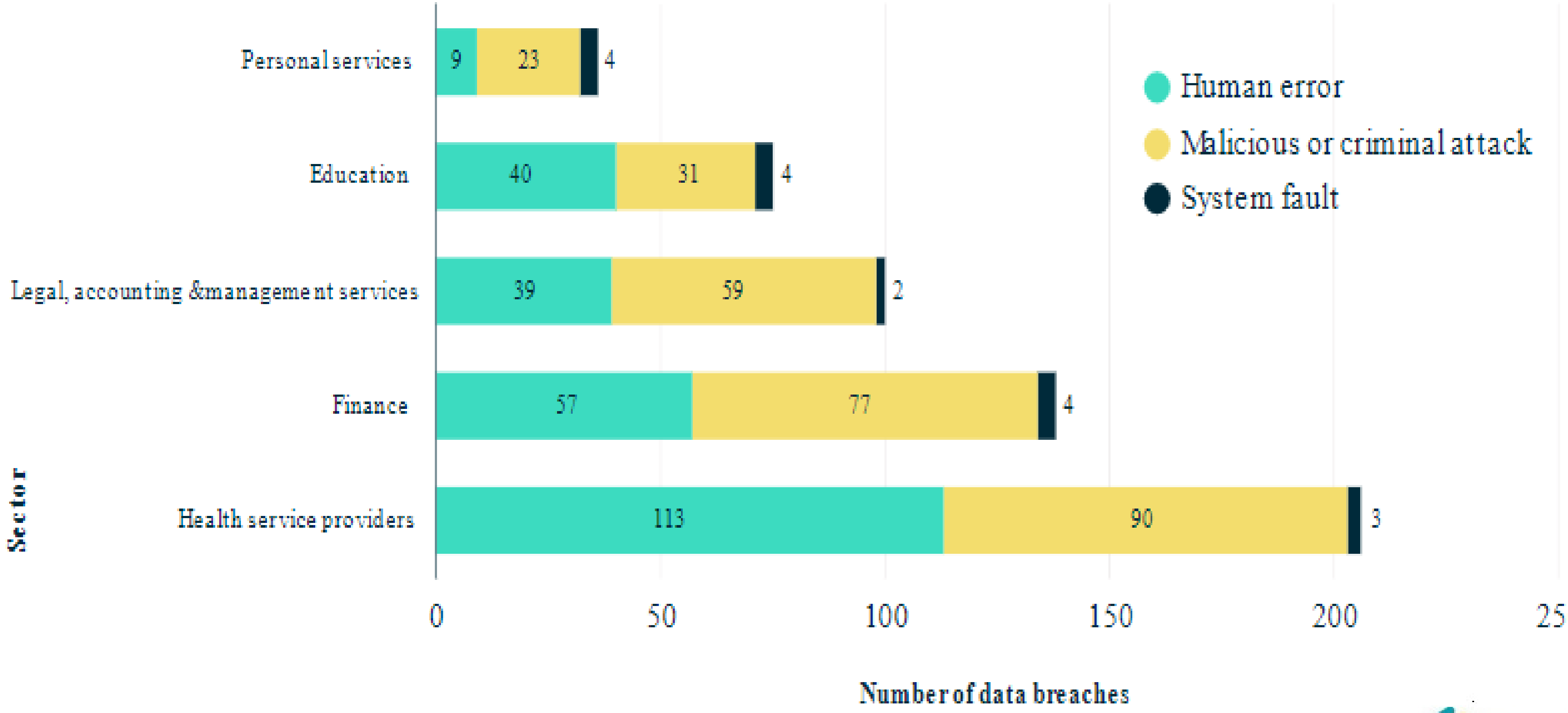
All Sectors from 1 April 2018 to 31 March 2019



LONMARK®

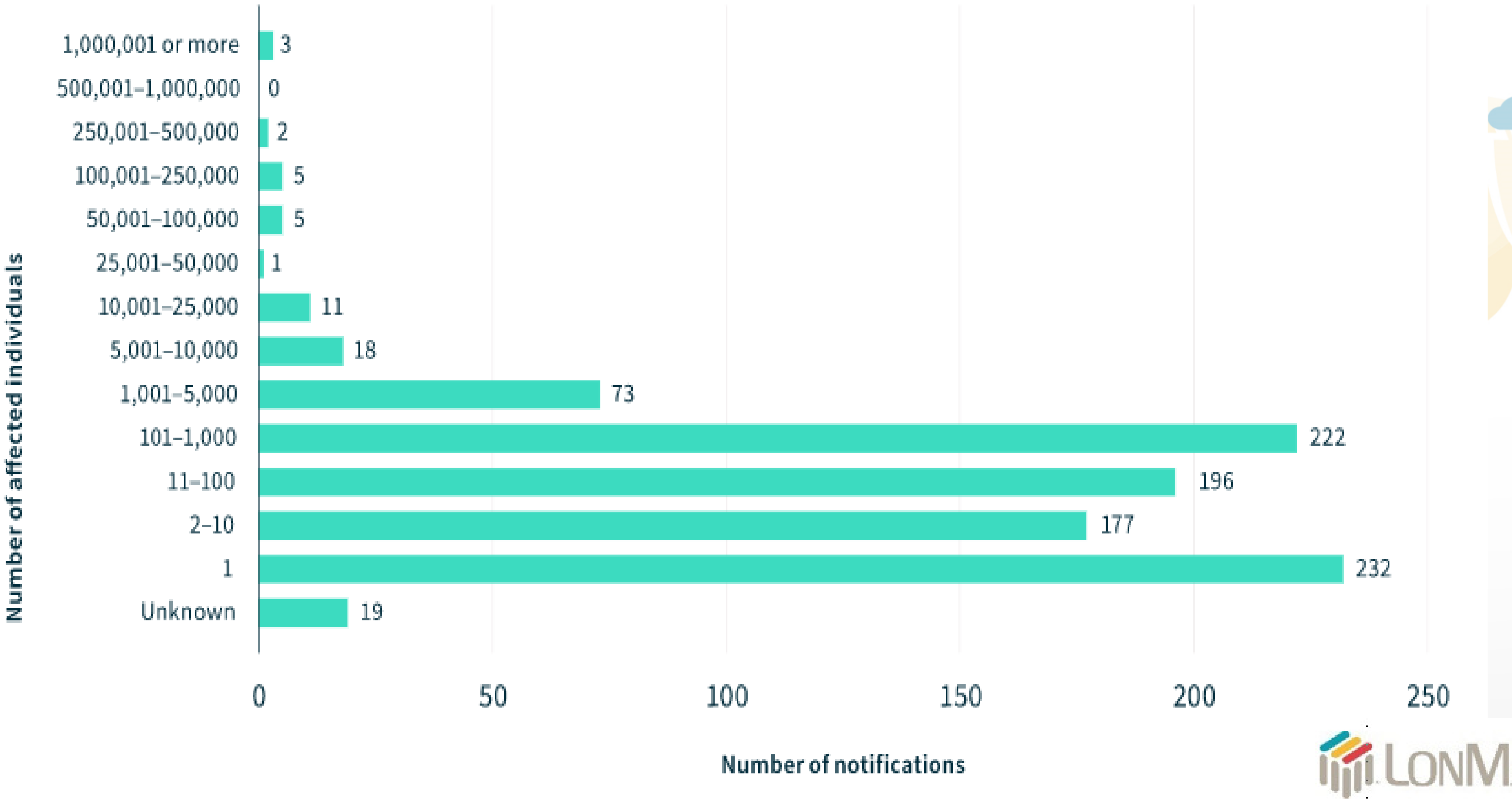
Top Reporting Sectors

All Sectors from 1 April 2018 to 31 March 2019



Number of Individuals Affected by Breaches

All Sectors from 1 April 2018 to 31 March 2019



Key Actions to Combat Cyber Attacks & Data Breaches

Cyber Security Check List

- Do we have Firewalls? What are the specific details?
- Do we have password management procedures? What are they?
- Do we protect all personally identifiable information through encryption?
- Are all laptops, phones and USBs password protected?
- Do we outsource handling of personally identifiable information, or store it in the cloud?
- Do we auto-update spyware and cybersecurity software?
- Are all business-critical systems and data information assets backed up to a second location, (eg. mirrored servers)?
- Have we had an audit of data security systems?
- If our IT network fails what would be the best impact on the operation of our business?
- Do we have a written data security policy and procedures communicated to all employees and do employees receive annual security awareness training?

LONMARK®

Cyber Security Check List

(Continued)

- Are we aware of any claims or circumstances that may be pending?
- What types of information do we hold, (eg; customer information, credit card numbers, 3rd party trade secrets or IP, medical or health care data, staff data)?
- Do we have a dedicated responsible person for data and IT management?
- Do we have a disaster recovery plan and/or business continuity plan and has it been tested in the last 18 months?
- Does our network include redundancy, resilience of any description to mitigate system interruptions or failures?
- Do we control or limit employee's ability to remove data from network or office?
- Does our website use web applications?
- Do we use monitored intrusion detection or intrusion protection systems?
- Are we aware of any instances of network intrusion highlighted in a security audit?
- Have we had unforeseen downtime to our servers of network of more than 12 hours?

Cyber Security Check List

(Continued)

- If we lose our system how long would it take us to get back up running?
- Do we require passwords to be changed regularly?
- Do we allow remote access to our internal network?
- Are all new payees and changes to existing payees' banking details authenticated with the client?
- Do transfers over 10K require a second signature or supervisor signoff?
- Are we entrusted with 3rd party funds?
- Have we ever suffered a crime of fidelity or computer crime loss?
- Do we have any joint ventures or consortia in place?
- If we lost our system how long would we want business interruption cover for?

Summary Guidelines

1. Contain
2. Assess
3. Take Remedial Action
4. Notify
5. Review

OAIC Notifiable Data Breach Scheme
12-month Insights Report

5 key focus areas are highlighted in the OAIC NDB Scheme 12-month Insights Report:

1. Your people and the role of training
2. Preventative technologies and processes
3. Preparation
4. Assessment of harm
5. Post-breach Communication