ACTUARIAL SOCIETY OF SOUTH AFRICA

QUANTIFYING RISK, ENABLING OPPORTUNITY

Subject:
Can You Afford Not To Invest In Cyber Security?

Author: Jaco Swanepoel
Organization: Absa Group Ltd
Date: 20 August 2019

Agenda

Can You Afford Not To Invest In Cyber Security?

1. **Cyber attacks can be sophisticated.**
2. **Financial implications are vast.**
3. **It's affecting people in the physical realm.**


SandWorm
LINKOS
group


Ooops, your important files are encrypted.
If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.
We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.
Please follow the instructions:
1. Send $300 worth of Bitcoin to following address:
1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX
2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:
hDgCcp-tDPRv9-TYEqag-1eps1H-6bqQko-EYQPYu-XHR665-CDXnNr-8kzCND-AYFkKu
If you already purchased your key, please enter it below.
Key: _

NotPetya had "negatively impacted third-quarter results, including an unfavorable revenue impact of approximately **$135 million** from lost sales and approximately **$175 million** in costs, spread across the cost of goods sold and the operating expense lines. We anticipate a similar impact to revenue and expenses in the fourth quarter, which is reflected in our updated guidance."

Merck CFO Robert Davis [Oct 2017]

https://www.techrepublic.com/article/notpetya-ransomware-outbreak-cost-merck-more-than-300m-per-quarter/

"Business volumes were negatively affected for a couple of weeks in July and as a consequence, our Q3 results will be impacted. We expect that the **cyber-attack** will impact results negatively by **$200-300m.**"

Mearsk [2017]

- Maersk is responsible for around 15 per cent of the world's entire shipping network.
- The company's entire network was down for days.

https://www.theregister.co.uk/2017/08/16/notpetya_ransomware_attack_cost_us_300m_says_shipping_giant_maersk/

"Operating results declined due to an estimated **$300 million** impact from the cyberattack, which was partially offset by the benefits from revenue growth, lower incentive compensation accruals and ongoing cost management initiatives."

FEDEX [2017]

http://investors.fedex.com/news-and-events/investor-news/news-release-details/2017/FedEx-Corp-Reports-First-Quarter-Earnings/default.aspx

NotPetya Totals

- **$10 billion** Total damages from NotPetya, as estimated by the White House
- **$870,000,000** Pharmaceutical company Merck
- **$400,000,000** Delivery company FedEx (through European subsidiary TNT Express)
- **$384,000,000** French construction company Saint-Gobain

https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

CYBER RISK AUGUST 5, 2019 / 8:28 PM / 3 DAYS AGO

North Korea took $2 billion in cyberattacks to fund weapons program: U.N. report

Michelle Nichols

4 MIN READ

UNITED NATIONS (Reuters) - North Korea has generated an estimated $2 billion for its weapons of mass destruction programs using "widespread and increasingly sophisticated" cyberattacks to steal from banks and cryptocurrency exchanges, according to a confidential U.N. report seen by Reuters on Monday.

The experts said they are investigating "at least 35 reported instances of DPRK actors attacking financial institutions, cryptocurrency exchanges and mining activity designed to earn foreign currency" in some 17 countries.

CYBER IS COMING.

ACTUARIAL SOCIETY OF SOUTH AFRICA

QUANTIFYING RISK, ENABLING OPPORTUNITY

Agenda

Can You Afford Not To Invest In Cyber Security?

1. **Cyber attacks can be sophisticated.**
2. **Financial implications are vast.**
3. **It's affecting people in the physical realm.**

Dylan Beattie
@dylanbeattie

- Hire a competent infosec team.
- We don't have budget for that.
- OK, be prepared to pay 1.5% of turnover in fines for each GDPR violation
- We don't have budget for that either.
- Well, golly. Sounds to me like you don't have a viable business model any more. Sorry about that.

♡ 1,102 1:49 AM - Jul 9, 2019 · Lewisham, London

352 people are talking about this

Marriott to be fined nearly £100m over GDPR breach

ICO imposes fine after personal data of 339 million guests was stolen by hackers

▲ Marriott said it would appeal against the fine. Photograph: Reuters

The international hotel group Marriott is to be fined almost £100m by the Information Commissioner's Office after hackers stole the records of 339 million guests.

British Airways faces $230 million fine. It would be a record under Europe's tough data privacy law

By Charles Riley, CNN Business

Updated 1500 GMT (2300 HKT) July 8, 2019

GDPR is officially out, how is the EU enforcing it?

Investors seek safe haven from trade war fears

Is a currency war coming?

Disney's streaming service will cost this much

London (CNN Business) – British Airways faces a record $230 million fine after a website failure compromised the personal details of roughly 500,000 customers.

Protection of Personal Information Act (PoPIA or POPI Act)

What steps will you have to take to comply?

Responsible parties will have to take various steps to comply. For example:

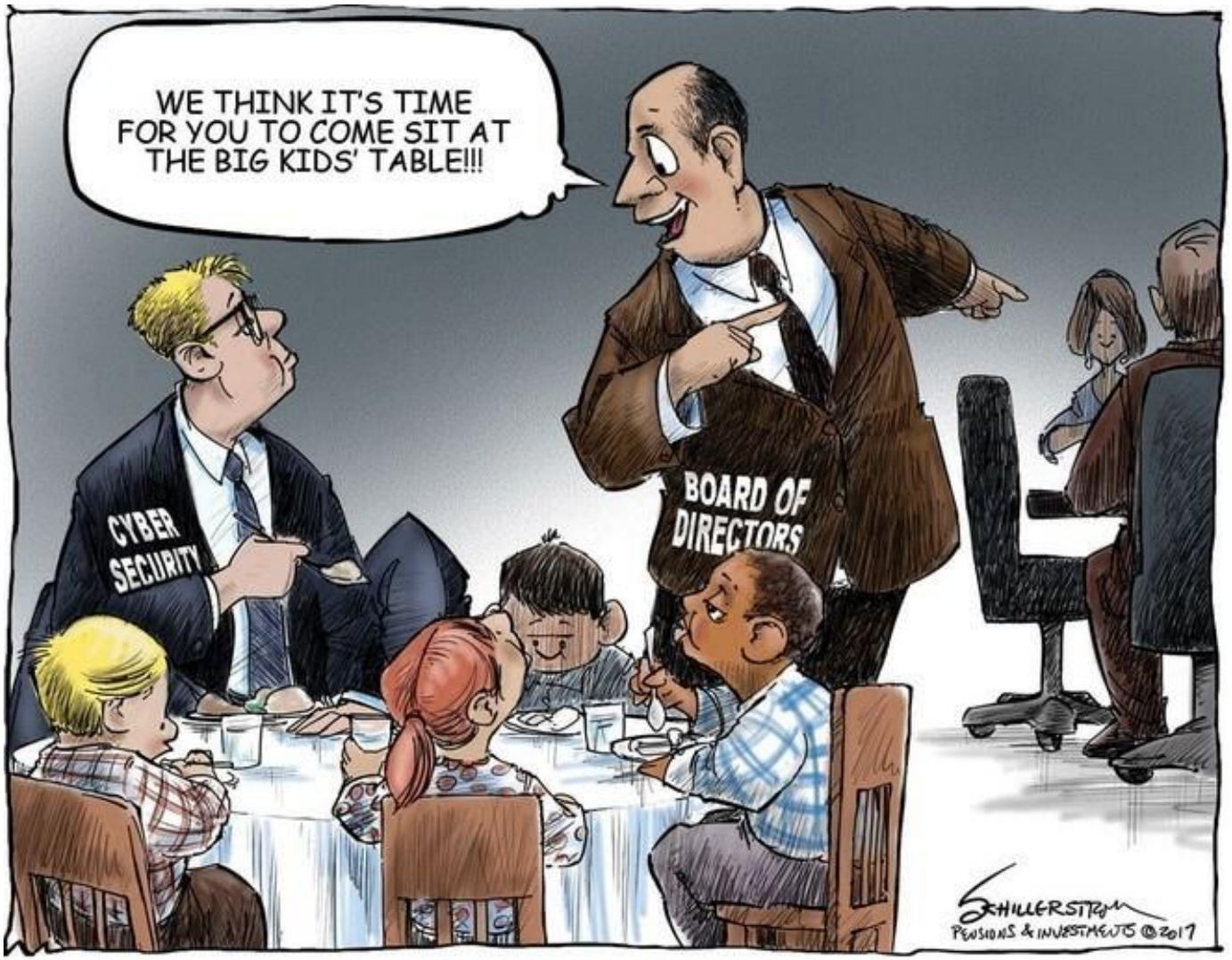
1. Appoint an Information Officer.
2. Draft a Privacy Policy.
3. Raise awareness amongst all employees.
4. Amend contracts with operators.
5. Report data breaches to the regulator and data subjects.
6. Check that they can lawfully transfer personal information to other countries.
7. Only share personal information when they are lawfully able to.

What are the Penalties for Non-compliance?

There are essentially two legal penalties or consequences for the responsible party:

1. A fine or imprisonment of between R1 million and R10 million or one to ten years in jail.
2. Paying money to data subjects to compensate them for the damage they have suffers.

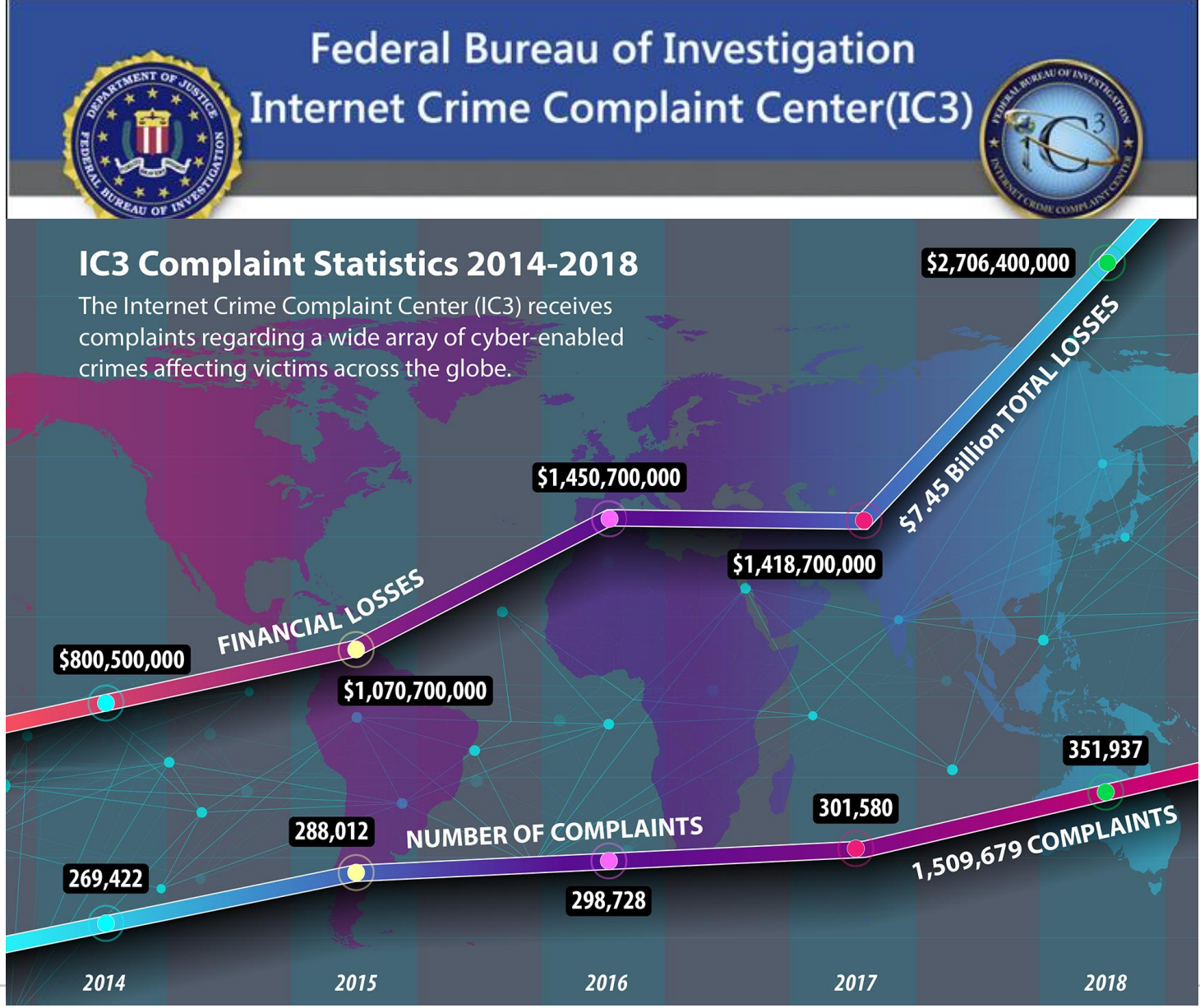

Jake Williams
@MalwareJake
If you have a business, and that business makes money, someone is going to target you eventually.
If you aren't doing cybersecurity because "we can't afford it" I have some very bad news for you: your business isn't really profitable anymore.
109 11:22 PM - Jul 20, 2019
45 people are talking about this


WE THINK IT'S TIME FOR YOU TO COME SIT AT THE BIG KIDS' TABLE!!!
CYBER SECURITY
BOARD OF DIRECTORS
SKILLERSTROM
PENSIONS & INVESTMENTS © 2017

RISKIQ®

ACTUARIAL SOCIETY OF SOUTH AFRICA

QUANTIFYING RISK, ENABLING OPPORTUNITY


Federal Bureau of Investigation
Internet Crime Complaint Center(IC3)
IC3 Complaint Statistics 2014-2018
The Internet Crime Complaint Center (IC3) receives complaints regarding a wide array of cyber-enabled crimes affecting victims across the globe.
$2,706,400,000
$7.45 Billion TOTAL LOSSES
$1,450,700,000
$1,418,700,000
FINANCIAL LOSSES
$800,500,000
$1,070,700,000
351,937
301,580
288,012
NUMBER OF COMPLAINTS
1,509,679 COMPLAINTS
269,422
298,728
2014
2015
2016
2017
2018

FBI IC3: Most Financial Costly Complaints

- Business Email Compromise
- Romance or Confidence Fraud
- Investment Scams

  (incl Ponzi and Pyramid schemes)

What is a data breach?

A data breach is defined as an event in which an individual's name and a medical record and/or a financial record or debit card is potentially put at risk, either in electronic or paper format. In our study, we identified three main causes of a data breach: malicious or criminal attack, system glitch or human error. The costs of a data breach vary according to the cause and the safeguards in place at the time of the data breach.

IBM – 2019 Cost of a Data Breach Report

IBM Security

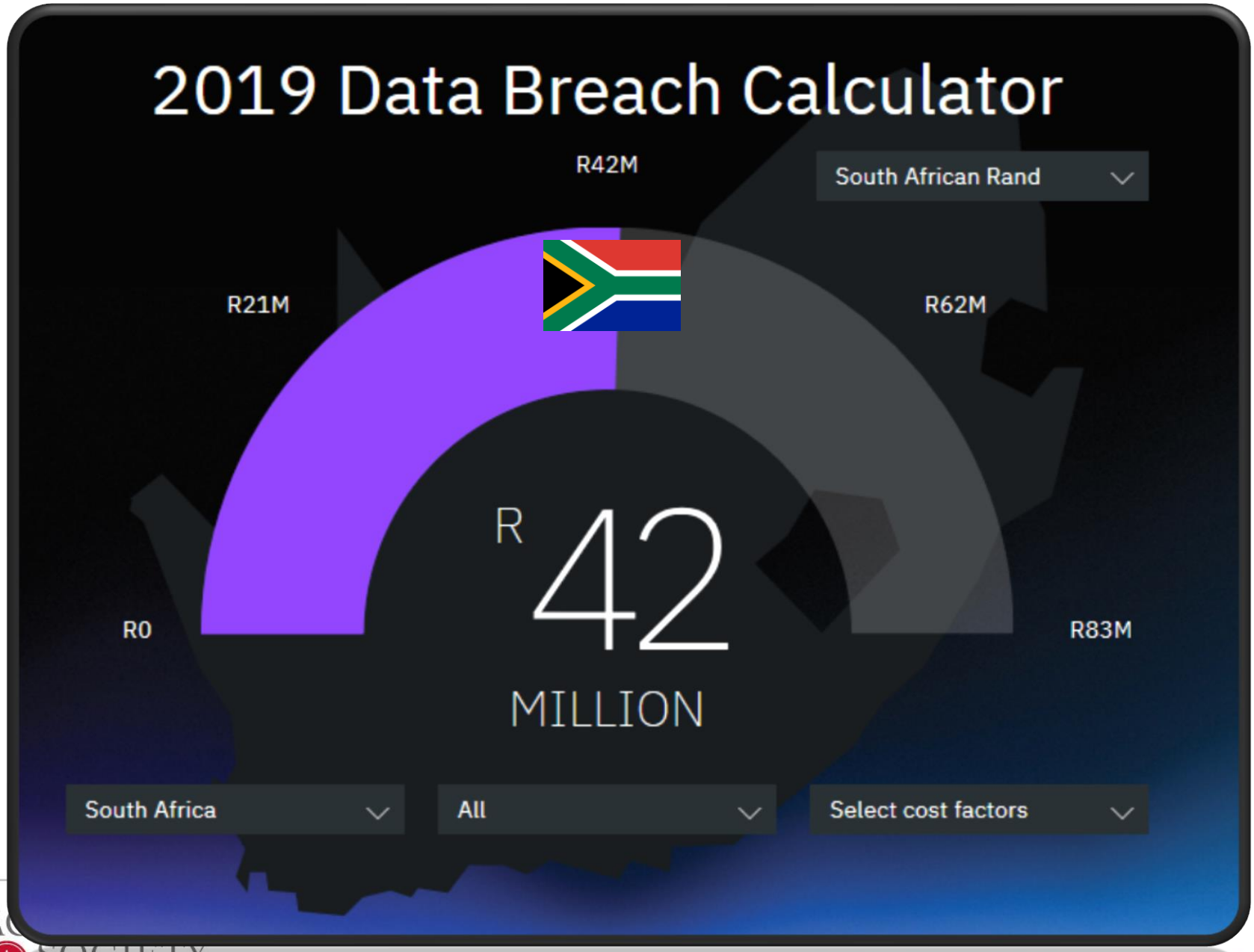
2019 Cost of a Data Breach Report

Global average total cost of a data breach

Measured in US$ millions

IBM

Ponemon INSTITUTE


2019 Data Breach Calculator
R42M
South African Rand
R21M
R62M
R0
R83M
R 42
MILLION
South Africa
All
Select cost factors

What Does Data Breaches Cost?

Detection and escalation

Activities that enable a company to detect and report a breach to appropriate personnel within a specified time period.

Examples:

- Forensic and investigative activities
- Assessment and audit services
- Crisis team management
- Communications to executive management and board of directors

Notification Costs

Activities that enable the company to notify individuals who had data compromised in the breach (data subjects) as regulatory activities and communications.

Examples:

- Emails, letters, outbound telephone calls, or general notice to data subjects that their personal information was lost or stolen
- Communication with regulators; determination of all regulatory requirements, engagement of outside experts

What Does Data Breaches Cost?

Post data breach response

Processes set up to help individuals or customers affected by the breach to communicate with the company, as well as costs associated with redress activities and reparation with data subjects and regulators.

Examples:

- Help desk activities / Inbound communications
- Credit report monitoring and identity protection services
- Issuing new accounts or credit cards
- Legal expenditures
- Product discounts
- Regulatory interventions (fines)

Lost business cost

Activities associated with the cost of lost business, including customer turnover, business disruption, and system downtime.

Examples:

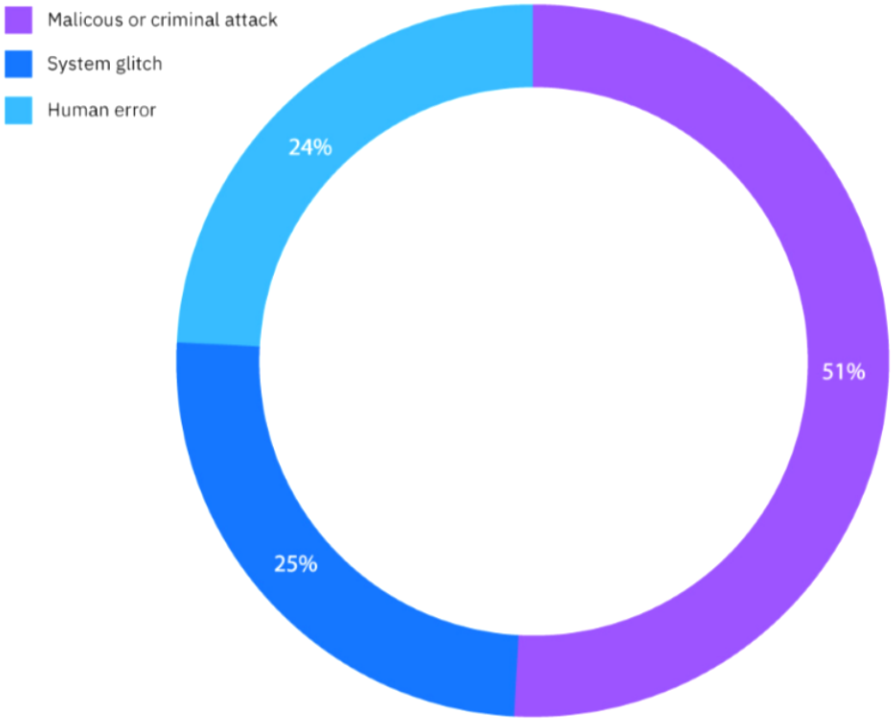
- Cost of business disruption and revenue losses from system downtime
- Cost of lost customers and acquiring new customers (customer turnover)
- Reputation losses and diminished goodwill

IBM Security

2019 Cost of a Data Breach Report

Malicious attacks are the leading cause of breaches

Breakdown of data breach root causes



IBM

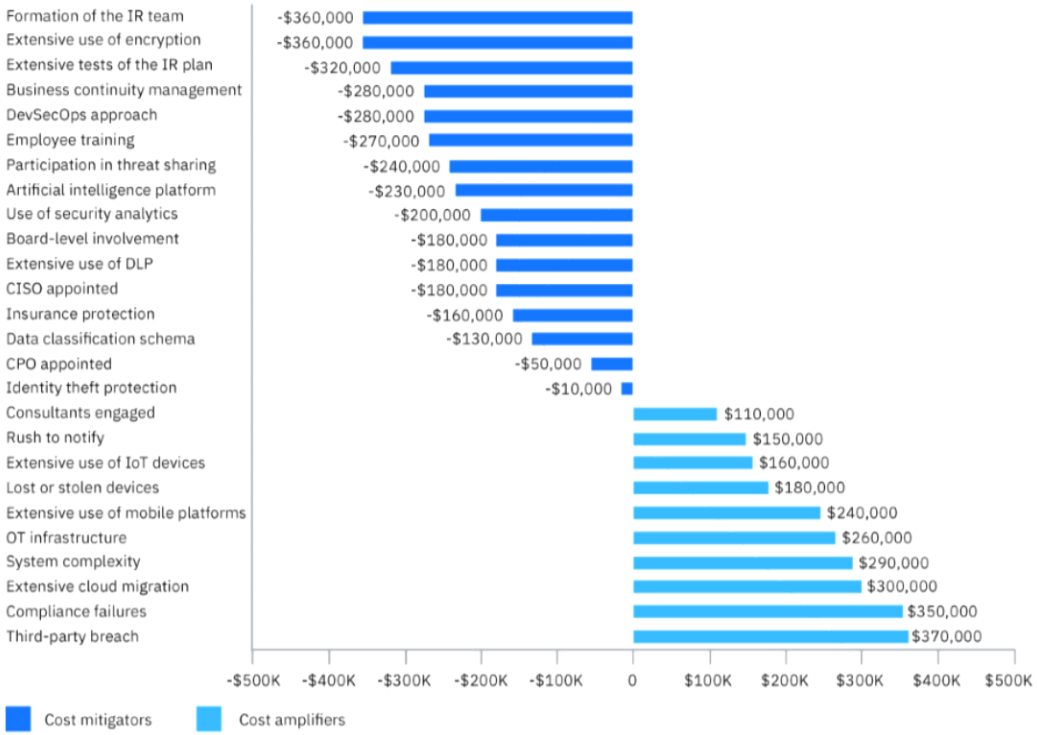
Ponemon INSTITUTE

IBM Security

2019 Cost of a Data Breach Report

How factors increase or decrease the total cost of a data breach

Difference from average total cost of US $3.92 million



IBM

Ponemon INSTITUTE

Agenda

Can You Afford Not To Invest In Cyber Security?

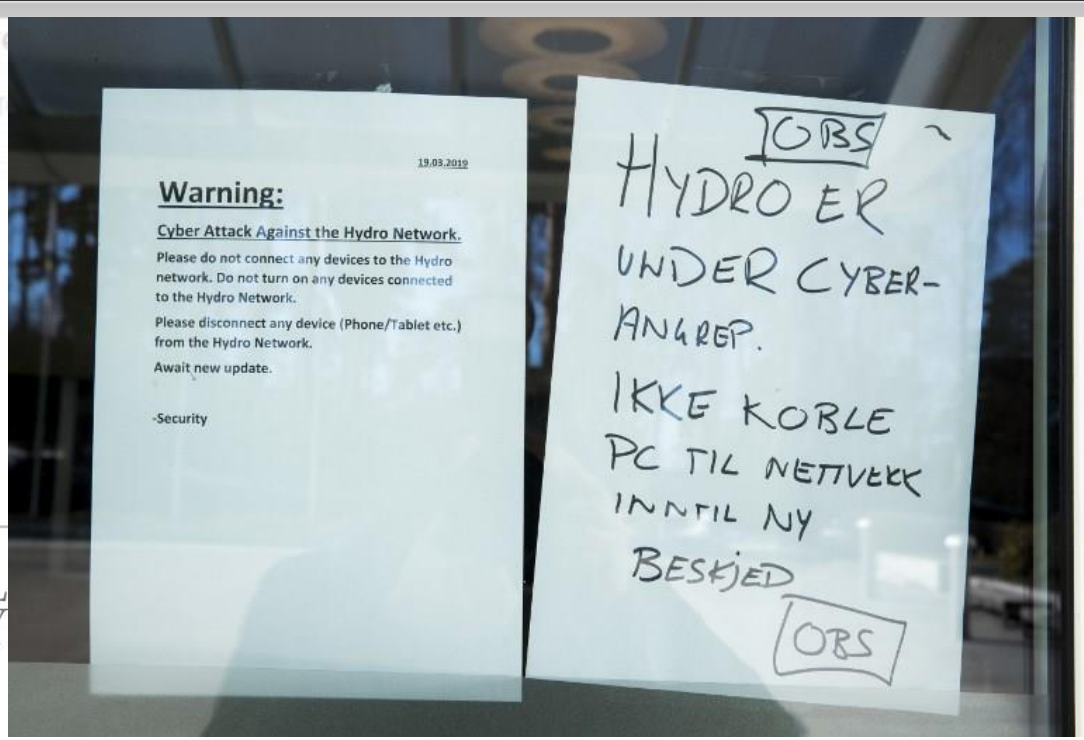
1. **Cyber attacks can be sophisticated.**
2. **Financial implications are vast.**
3. **It's affecting people in the physical realm.**

Aluminum maker Hydro battles to contain ransomware attack

Gwladys Fouche, Terje Solsvik

5 MIN READ

OSLO (Reuters) - Norsk Hydro, one of the world's largest aluminum producers, battled on Tuesday to contain a cyber attack which halted parts of its production, the latest example of the damage hackers can cause to business and industry.




@CityPowerJhb
@CityPowerJhb
#Update City Power has been hit by a Ransomware virus. it has encrypted all our databases, applications and network. Currently our ICT department is cleaning and rebuilding all impacted applications.^GR
112 8:30 AM - Jul 25, 2019
250 people are talking about this

@CityPowerJhb @CityPowerJhb · Jul 25, 2019

#Update City Power has been hit by a Ransomware virus. it has encrypted all our databases, applications and network. Currently our ICT department is cleaning and rebuilding all impacted applications.^GR

@CityPowerJhb
@CityPowerJhb

Customers may not be able to visit our website and may not be able to buy electricity units until our ICT department has sorted the matter out, Customers and stakeholders will be updated as and when new information becomes available^GR

♡ 21 8:33 AM - Jul 25, 2019

Haley @BellaNymph · Jul 25, 2019

@CityPowerJhb is there a problem with your system to buy electricity? Been trying since 8pm via STD bank and FNB and neither are working!!!

Haley
@BellaNymph

@CityPowerJhb please an update???? This is getting ridiculous. We have exotic fish in a fish tank that need their air filter on!!

8:18 AM - Jul 25, 2019

Baltimore ransomware attack will cost the city over $18 million

City residents are still facing issues.

Essential services like police, fire and EMTs have remained operational but the attack has affected hospitals, factories producing vaccines, airports and ATMs.

For example, some systems are still dependent on inefficient manual workarounds. The city's water billing systems are offline so residents may face larger than usual water bills, and parking or speeding fines can only be paid using paper tickets instead of electronic methods.

https://www.engadget.com/2019/06/06/baltimore-ransomware-18-million-damages/

Professional Services Contracts Related to Ransomware

Ransomware dollars spent on six security consultant firms to complete forensic analysis and detection on workstations,
network devices, servers, and databases. These firms also assisted in the hardening overall and overall protection of
Baltimore City's computing environment.

$2,810,575

Baltimore City partnered with the following vendors: FireEye INC., Clark Hill PLC., Seculore Solutions LLC., Dyn Tek Services LLC., Microsoft, and Crypsis Digital Security LLC DBA: Crypsis Group.

Ransomware dollars spent on computer technicians that deployed workstation, laptops and replacement hard drives for ransomware impacted devices. The State of Maryland also contributed technicians to help with these tasks.

$485,755

Ransomware dollars spent for staff augmentation overtime (for existing staff) and expertise for several infrastructure tools.

$111,742

Equipment Purchases Related to Ransomware

Dollars spent on the purchase of hardware (workstation, monitors etc.) and software related to ransomware recovery.

$1,902,474

Total Professional Services and Equipment Contract Costs to date **$5,310,546**

Contract costs incurred as of 7/11/2019

https://mayor.baltimorecity.gov/city-baltimore-faq

Ransomware infection takes some police car laptops offline in Georgia

Ransomware infection impacted police car laptops for the Georgia State Patrol, Georgia Capitol Police, and the Georgia Motor Carrier Compliance Division.

By Catalin Cimpanu for Zero Day | July 29, 2019 -- 22:17 GMT (23:17 BST) | Topic: Security

A ransomware infection at the Georgia Department of Public Safety (DPS) has crippled laptops installed in police cars across the state.

MORE FROM CATALIN CIMPANU

Security
Researchers find security flaws in 40 kernel drivers from 20 vendors

Security
Clever attack uses SQLite databases to hack other apps, malware servers

Security
Microsoft names top security researchers, zero-day contributors

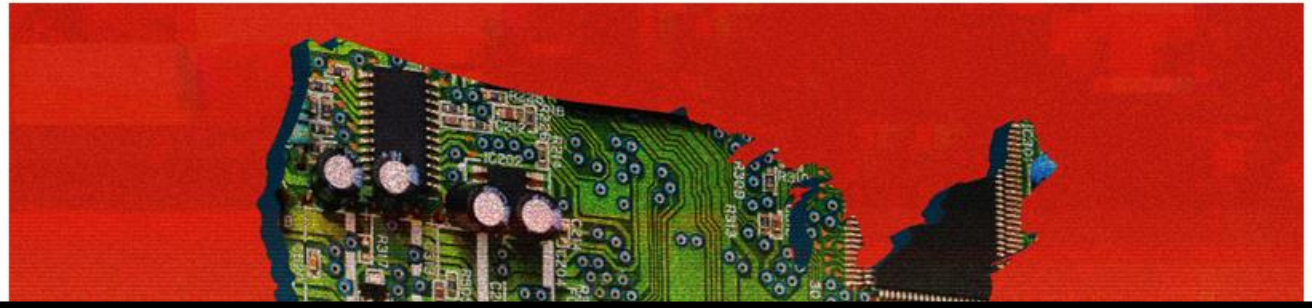
Security
Apple expands bug bounty to macOS, raises bug rewards

NEWSLETTERS

A Florida city paid a $600,000 bitcoin ransom to hackers who took over its computers — and it's a massive alarm bell for the rest of the US

SINÉAD BAKER
JUN 20, 2019, 8:01 PM

FACEBOOK TWITTER REDDIT LINKEDIN EMAIL



- A Florida city agreed to pay $US600,000 worth of bitcoin to hackers who took its computer systems offline with a cyberattack.
- Riviera Beach's city council voted to pay the money after an attack in May affected the city's online services, including email and 911 dispatches.
- The attack is part of a pattern that has targeted cities around the US. The disruption has cost millions of dollars.

https://www.businessinsider.com.au/florida-city-paid-600k-hackers-shows-us-unprepared-for-threat-2019-6?r=US&IR=T

Florida city fires IT employee after paying ransom demand last week

At least one head rolls after second Florida city pays gigantic ransom demand to ransomware gang.

By Catalin Cimpanu for Zero Day | July 1, 2019 -- 17:25 GMT (18:25 BST) | Topic: Security

Officials from Lake City, Florida, have fired an IT employee last week after the city was forced to approve a gigantic ransomware payment of nearly $500,000 last Monday.

The employee, whose name was not released, was fired on Friday, according to local media reports [1, 2], who cited the Lake City mayor.

Agenda

Can You Afford Not To Invest In Cyber Security?

1. **Cyber attacks can be sophisticated.**
2. **Financial implications are vast.**
3. **It's affecting people in the physical realm.**

Thank You