Document Classification: CSCS Controlled

CSCS
RC 201018
CENTRAL SECURITIES CLEARING SYSTEM PLC

Cyber Vigilance

Easiest but Most Potent Cybersecurity Tool

Tobe Nnadozie
Divisional Head, Technology and Innovations

September 2020

Speaker's Profile

Tobe Nnadozie

Tobe is passionate about innovation and has been a major part of the transformation of 4 highly innovative institutions in Nigeria including GTBank, Wapic Insurance, FCMB, Stanbic IBTC, Heritage Bank and others. He is also involved in a number of FINTECH groups and firms where he provides advisory services and take-off investment. He is a lover of classical music and plays the clarinet and some piano.

Education

B.Sc. Physics Electronics
Masters in IT
Masters in Business Admin.
Fellow, British Computer Society
Associate – CIB, Scotland
Associate – CIB, Nigeria

Experience

Divisional Head, Technology & Innovation – CSCS Plc
Head, Digital & Tech – Wapic Insurance
Group CIO – Wapic Insurance
Divisional Head, Innovations & Products – Heritage Bank
CIO – Axa Mansard Insurance

Extras

Board, Cyber Security Org.
Leadership and Mentoring
Enterprise Architecture
Youth Empowerment
SMEs Empowerment.

The Journey Map

01

Firstly …

02

The Facts

03

The Foundations

04

The Fix

05

… Finally

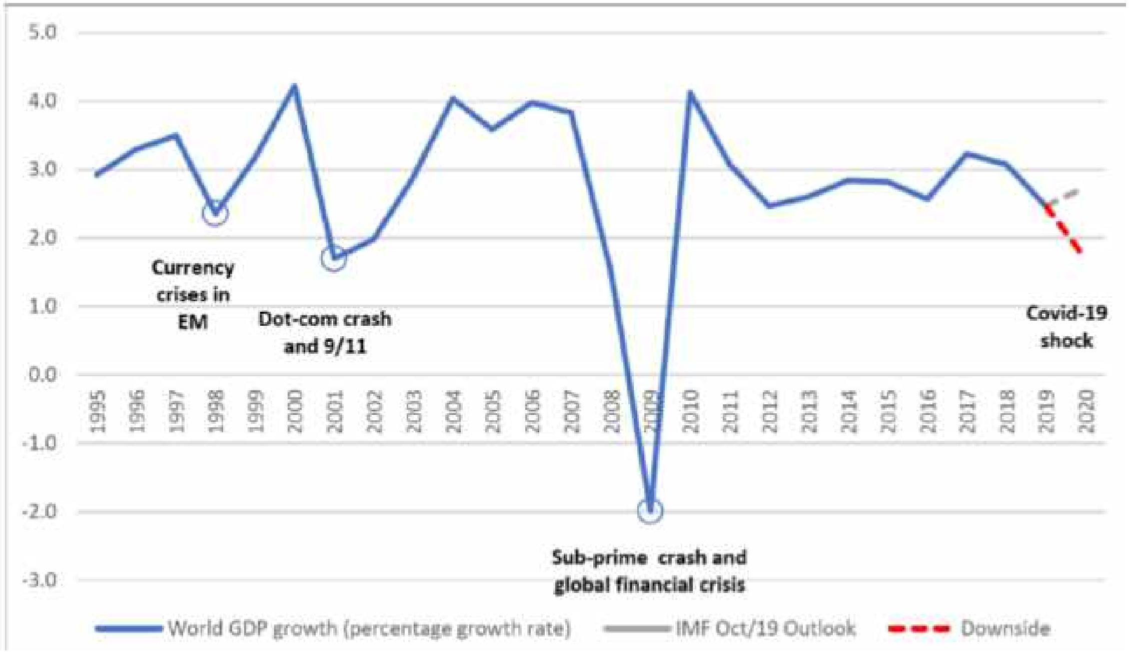
ed

1

First of all …

Cyber Security, Cyber Fencing, Cyber Citizens, Cyber Policing … and then Covid

Economic Impact of Covid



Source: United Nations

- With the exception of the Sub Prime Crash that resulted into the Global Financial Markets, this is expected to be the worst negative impact on GDP globally in the lifetime of most adults.
- McKinsey estimates that job losses in the UK could be 7.6million people due to Covid.
- NBS in Nigeria estimates that between 79% of businesses were impacted by Covid. Recall that Nigeria has about 40m SMEs, majority that could not trade

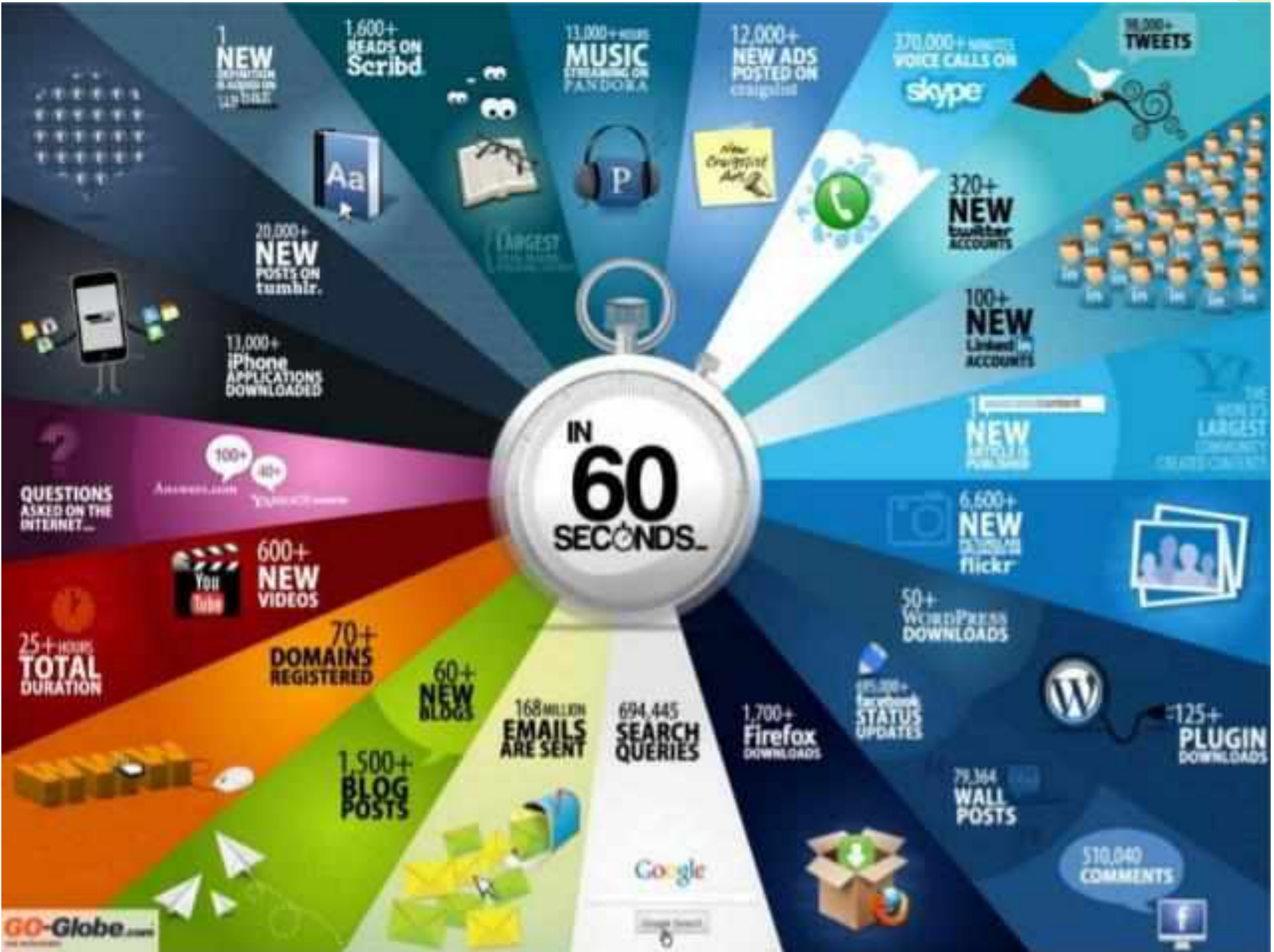
Why Cyber Crime?

- Survival
- Security
- Stability
- Success

- Sabotage
- Scandals
- Scorn
- Selfishness

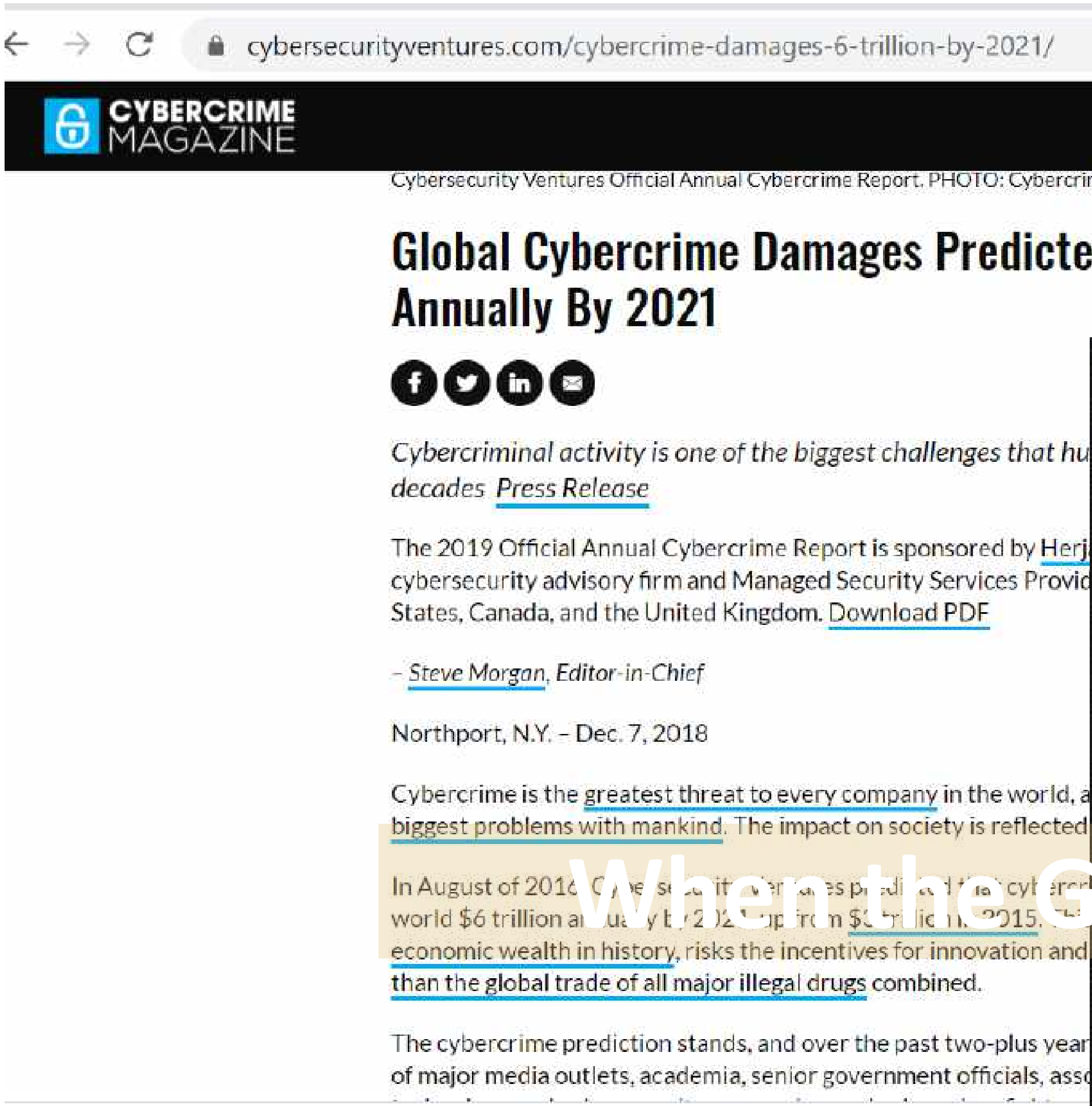
SURVIVAL

Is the World learning better from CyberCriminals?


IN 60 SECONDS...
1 NEW DEFINITION IS ADDED ON URBAN DICTIONARY
1,600+ READS ON Scribd
13,000+ HOURS MUSIC STREAMING ON PANDORA
12,000+ NEW ADS POSTED ON craigslist
New Craigslist Ad
370,000+ MINUTES VOICE CALLS ON skype
98,000+ TWEETS
320+ NEW twitter ACCOUNTS
100+ NEW LinkedIn ACCOUNTS
1 NEW ARTICLE IS PUBLISHED
THE WORLD'S LARGEST COMMUNITY CREATED CONTENT
6,600+ NEW PICTURES ARE UPLOADED ON flickr
50+ WORDPRESS DOWNLOADS
125+ PLUGIN DOWNLOADS
695,000+ facebook STATUS UPDATES
79,364 WALL POSTS
510,040 COMMENTS
1,700+ Firefox DOWNLOADS
694,445 SEARCH QUERIES
Google
Google Search
168 MILLION EMAILS ARE SENT
1,500+ BLOG POSTS
60+ NEW BLOGS
70+ DOMAINS REGISTERED
25+ HOURS TOTAL DURATION
600+ NEW VIDEOS
You Tube
100+ Answers.com
40+ YAHOO! Answers
QUESTIONS ASKED ON THE INTERNET...
13,000+ iPhone APPLICATIONS DOWNLOADED
20,000+ NEW POSTS ON tumblr.
Aa
GO-Globe.com

It is a whole NEW world of HYPER-CONNECTIONS

When the Going was Good



cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

Cybersecurity Ventures Official Annual Cybercrime Report. PHOTO: Cybercrime Magazine.

Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021

Cybercriminal activity is one of the biggest challenges that hu decades *Press Release*

The 2019 Official Annual Cybercrime Report is sponsored by Herj cybersecurity advisory firm and Managed Security Services Provid States, Canada, and the United Kingdom. Download PDF

– *Steve Morgan, Editor-in-Chief*

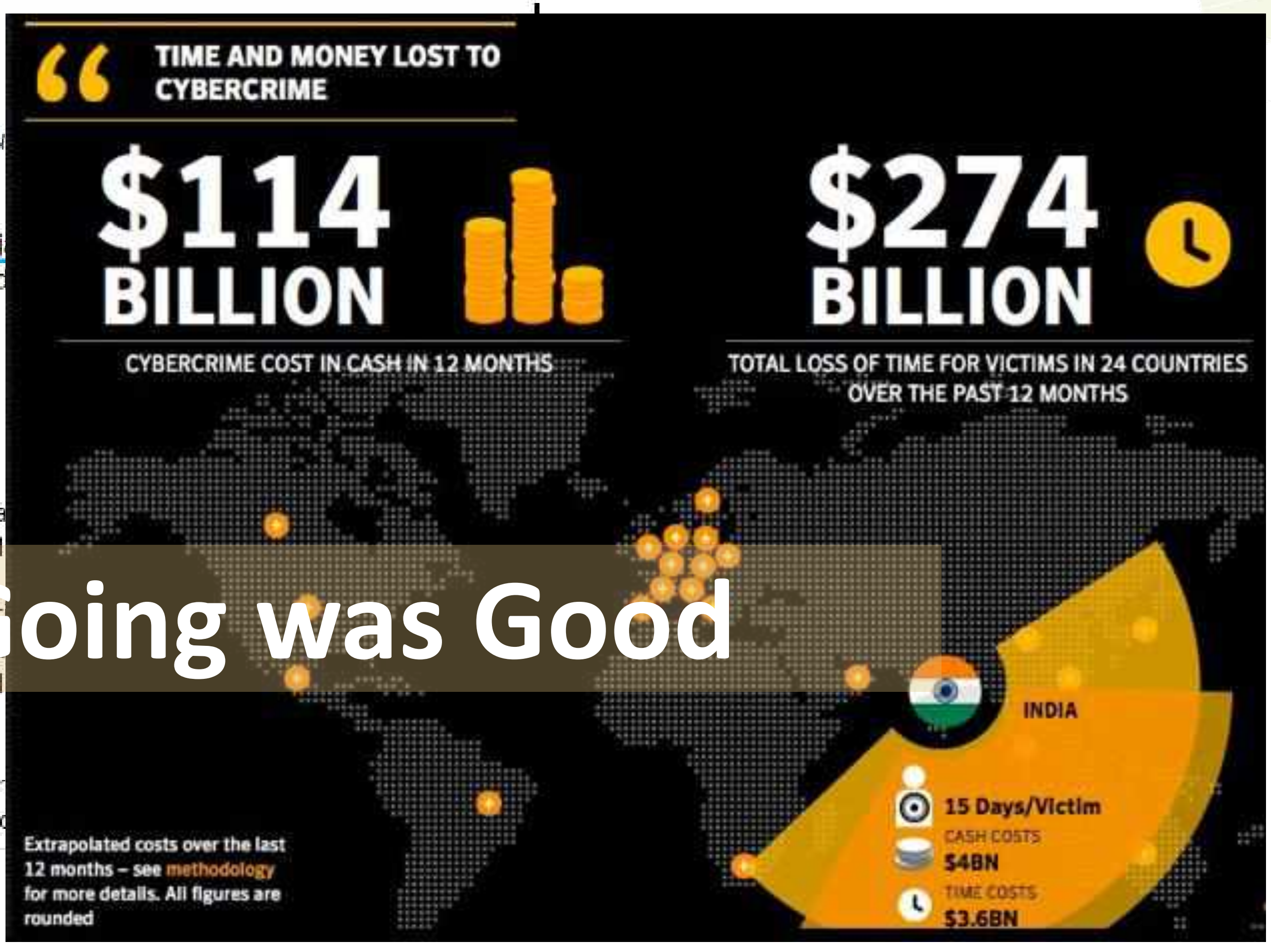
Northport, N.Y. – Dec. 7, 2018

Cybercrime is the greatest threat to every company in the world, a biggest problems with mankind. The impact on society is reflected

In August of 2016 Cybersecurity Ventures predicted that cybercrime world $6 trillion annually by 2021, up from $3 trillion in 2015. Thi economic wealth in history, risks the incentives for innovation and than the global trade of all major illegal drugs combined.

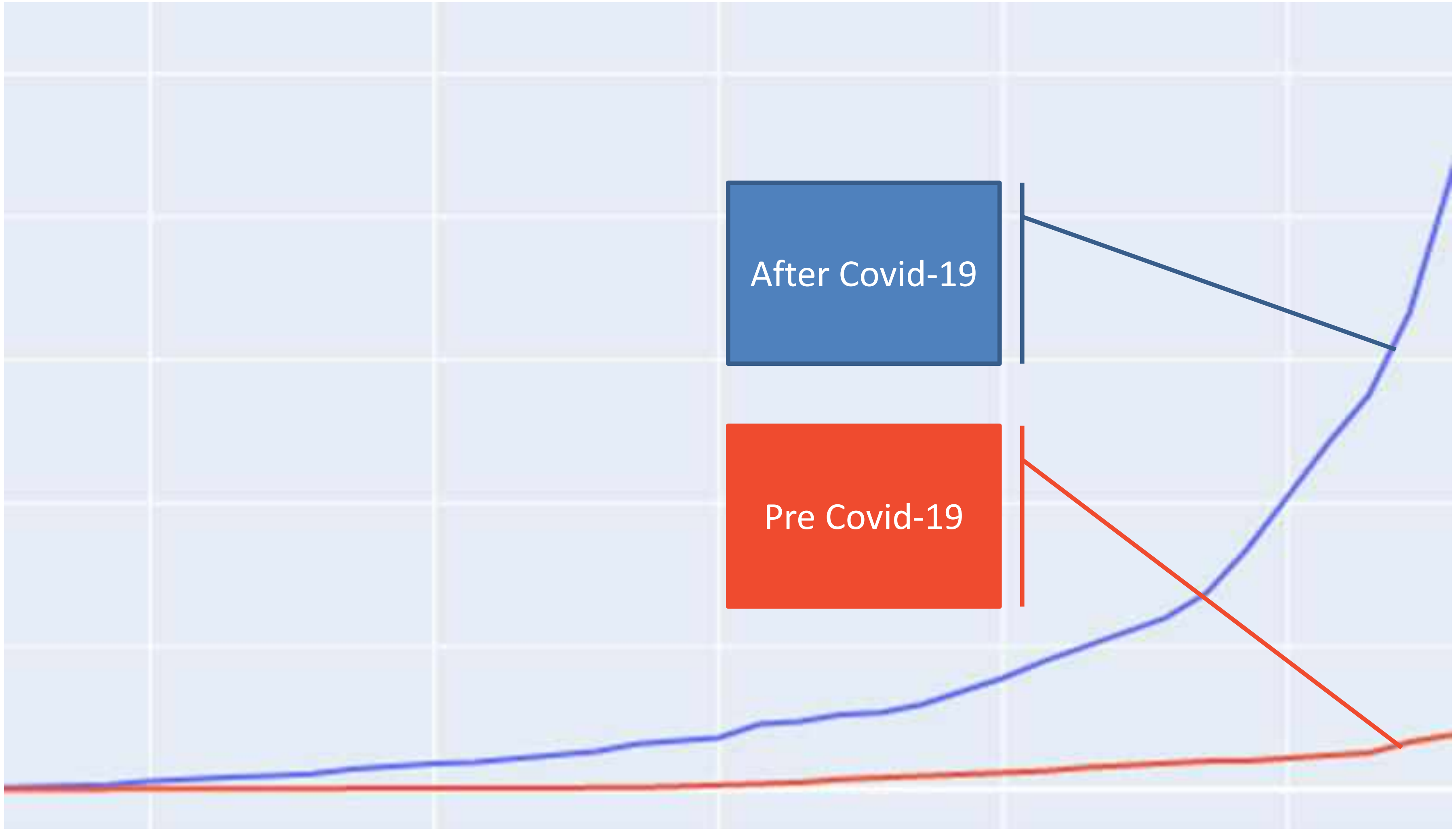
The cybercrime prediction stands, and over the past two-plus year of major media outlets, academia, senior government officials, asso

Source: CyberCrime Magazine



Source: CyberEdge 2020 Cyberthreat Defense Report

EW
NORMAL

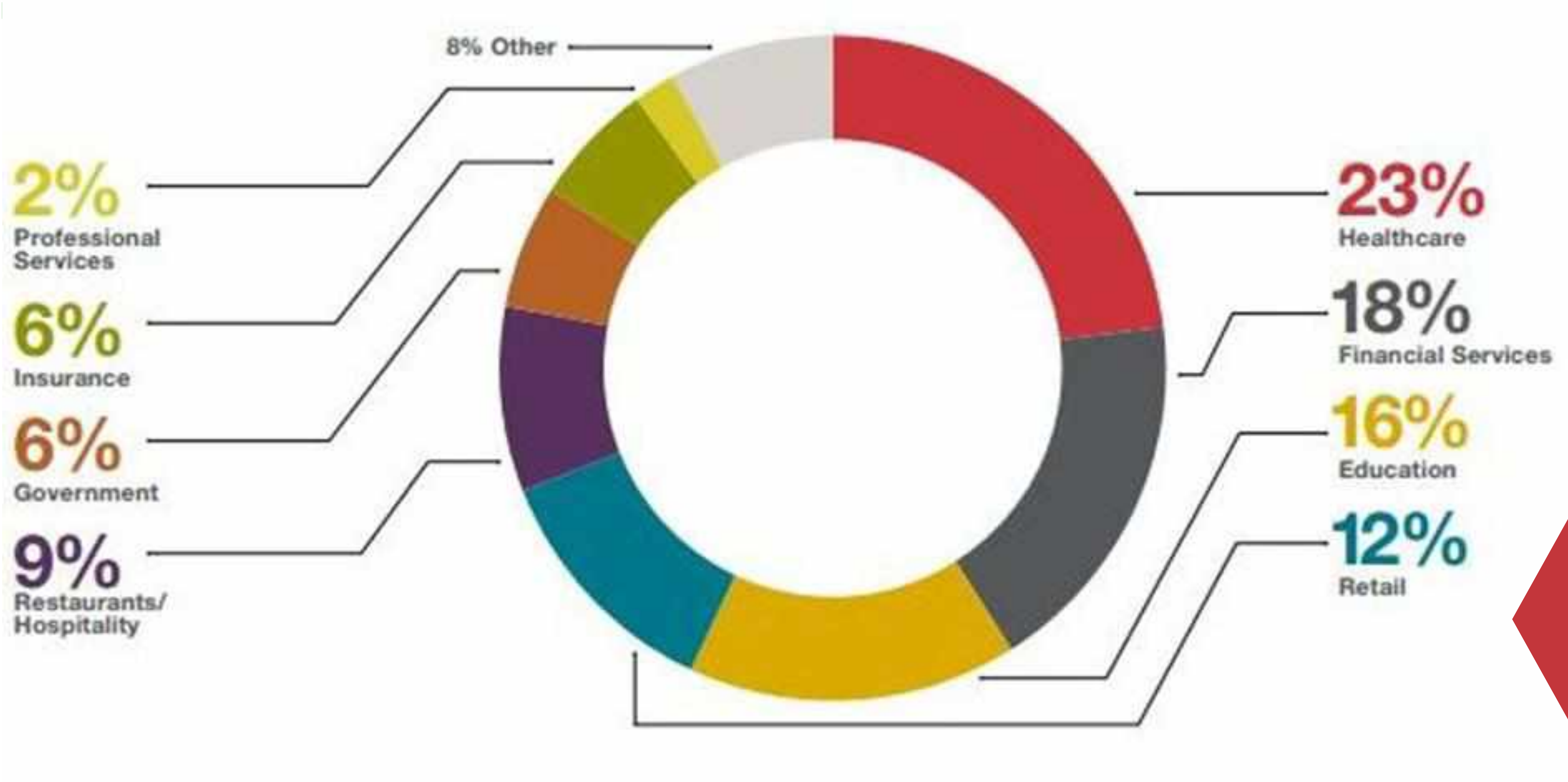


As the Going keeps Going…

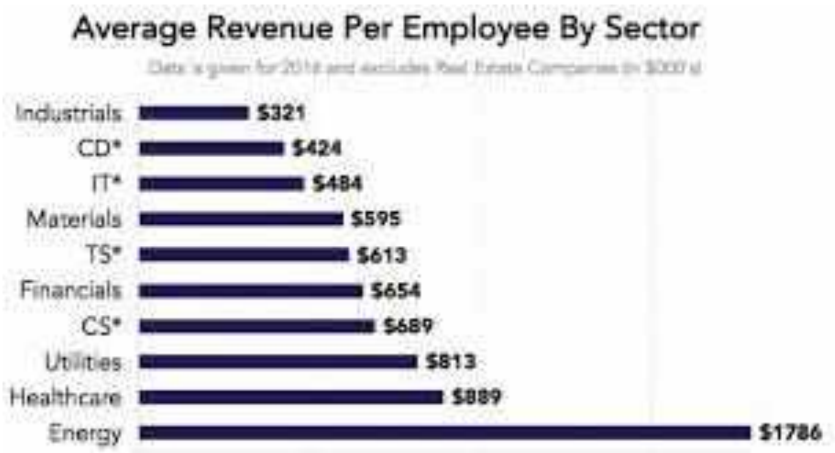
2

The Facts

Some interesting facts about Cyber Crimes and Myth ‘Debunkers’

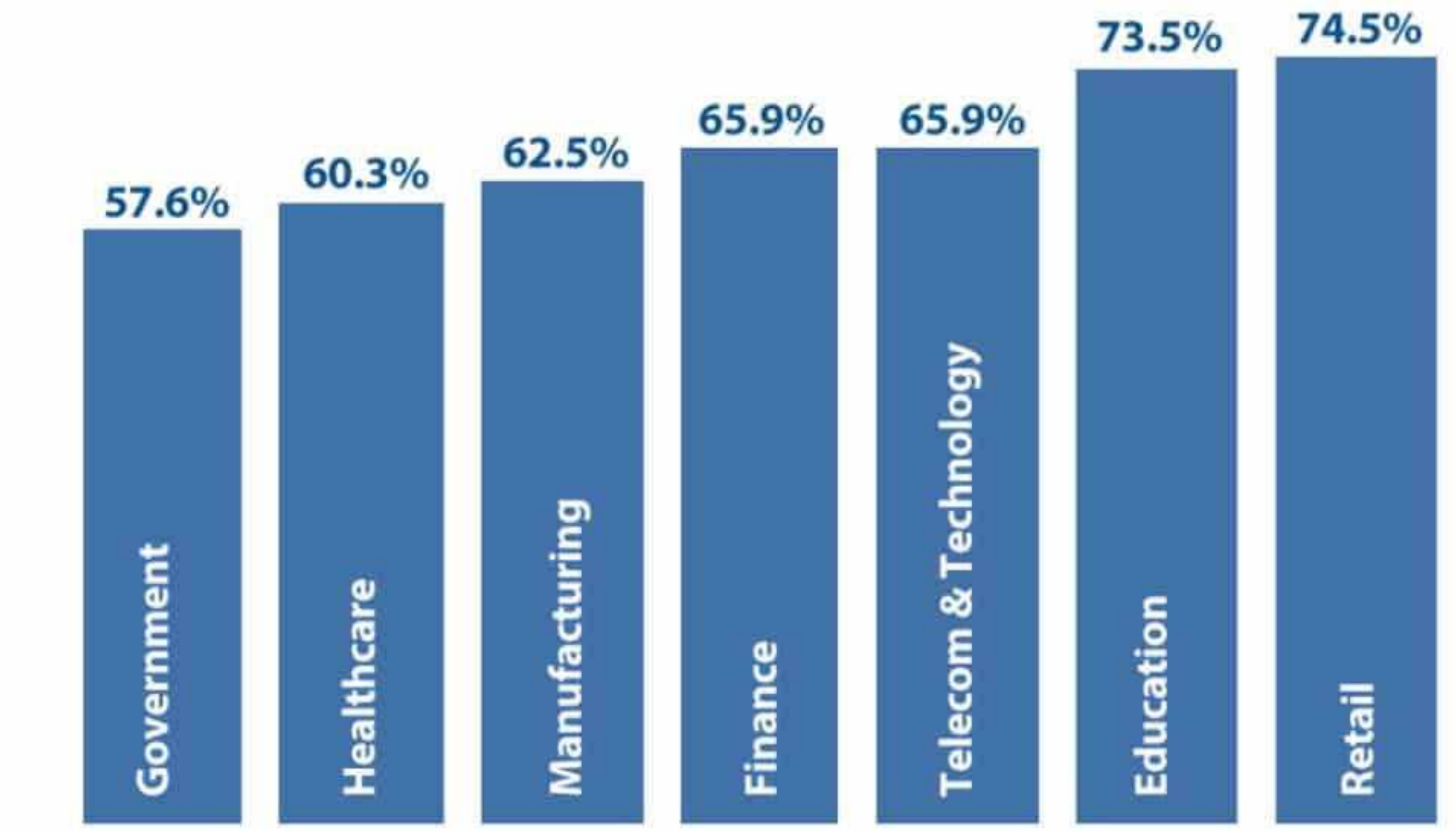


Industries affected by Data Breaches
Source: www.premierinsurancecorp.com



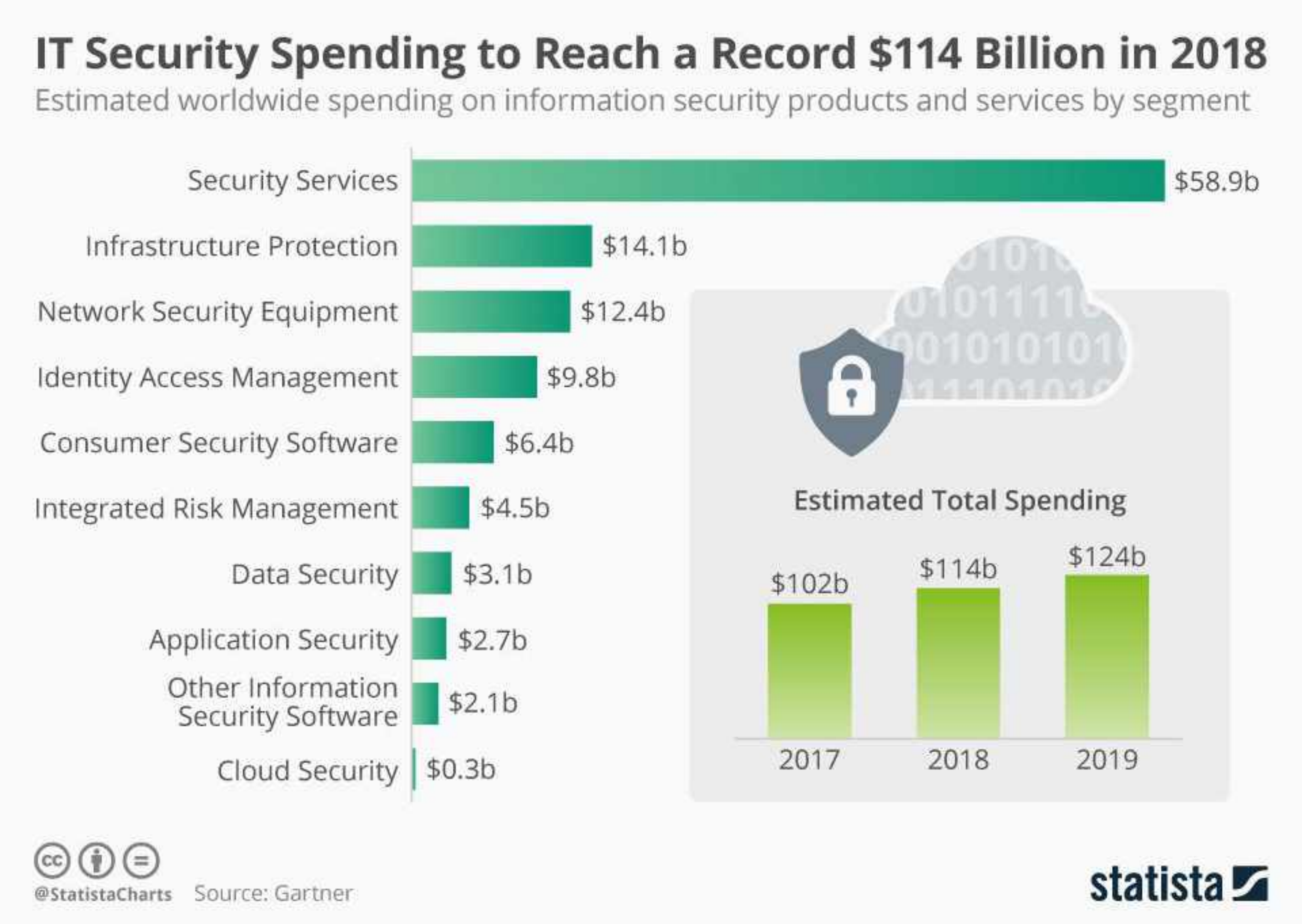
Cyber-attack is worsening and the targets are industries with highest income or automation globally

Where is Cyber Security Compromise Expected over the Next 12 Months



Compromise seems to be a growing concern of everyone and the fact is that all projections show that this will affect all sectors especially the retail and financial services sectors

Source: CyberCrime Magazine

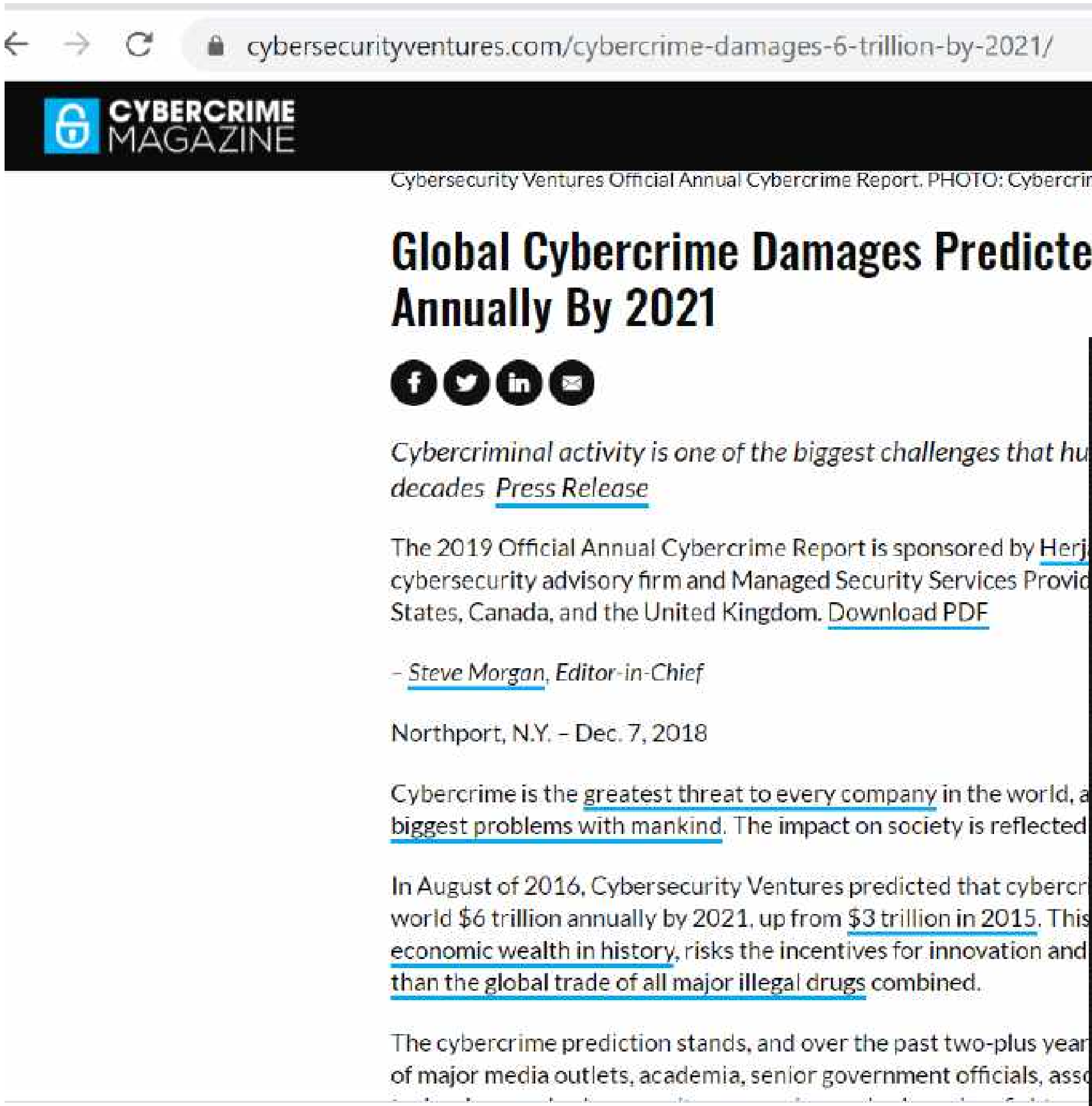


IT Security Spending to Reach a Record $114 Billion in 2018

Estimated worldwide spending on information security products and services by segment

Source: Gartner

The pattern of spend on security show clearly that organizations are doing all they can to ensure they are more secured



cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

CYBERCRIME MAGAZINE

ABOUT RESEARCH LISTS VI

Cybersecurity Ventures Official Annual Cybercrime Report. PHOTO: Cybercrime Magazine.

Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021

Cybercriminal activity is one of the biggest challenges that hu
decades *Press Release*

The 2019 Official Annual Cybercrime Report is sponsored by Herj
cybersecurity advisory firm and Managed Security Services Provid
States, Canada, and the United Kingdom. Download PDF

– *Steve Morgan, Editor-in-Chief*

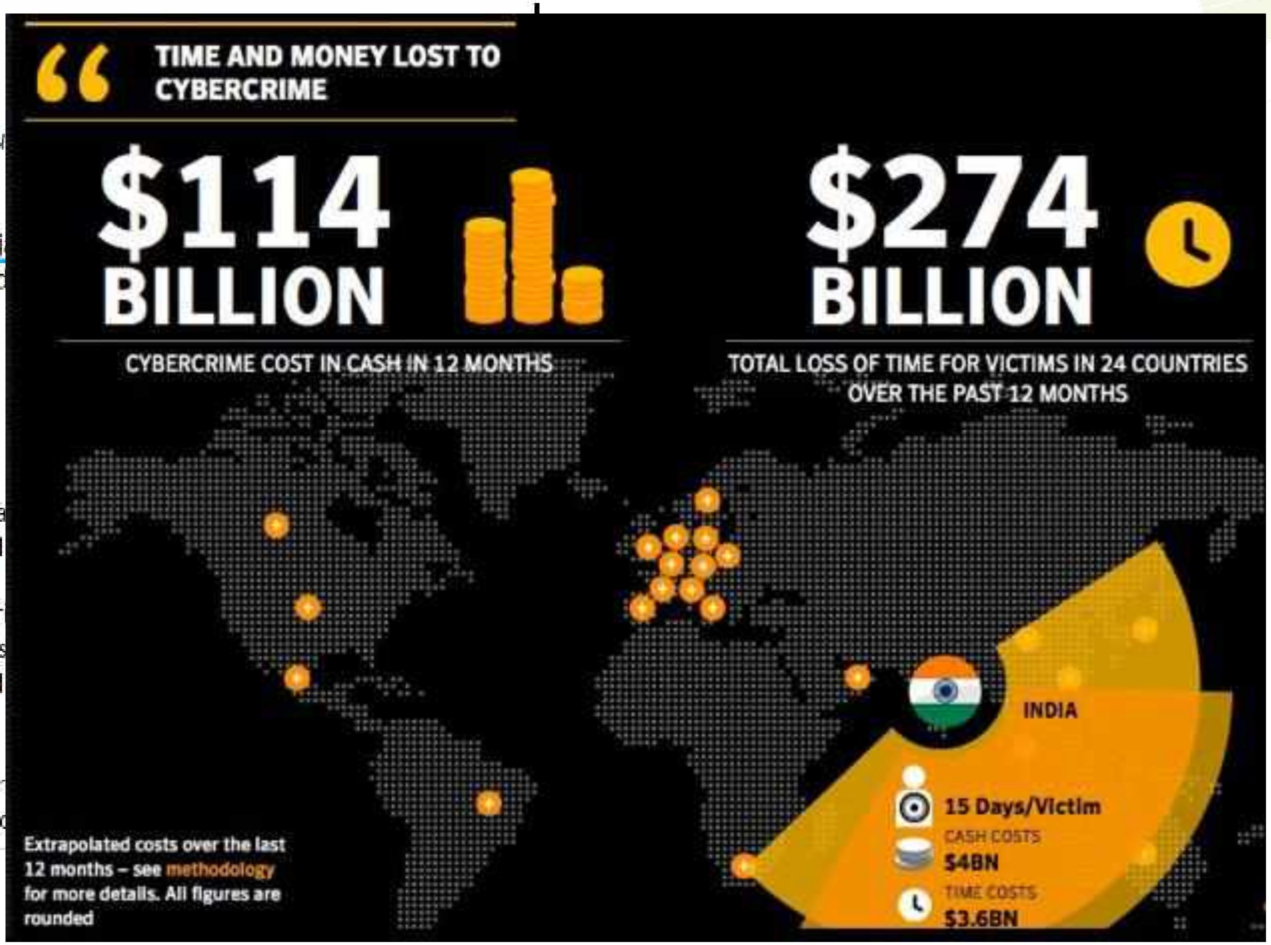
Northport, N.Y. – Dec. 7, 2018

Cybercrime is the greatest threat to every company in the world, a
biggest problems with mankind. The impact on society is reflected

In August of 2016, Cybersecurity Ventures predicted that cybercr
world $6 trillion annually by 2021, up from $3 trillion in 2015. This
economic wealth in history, risks the incentives for innovation and
than the global trade of all major illegal drugs combined.

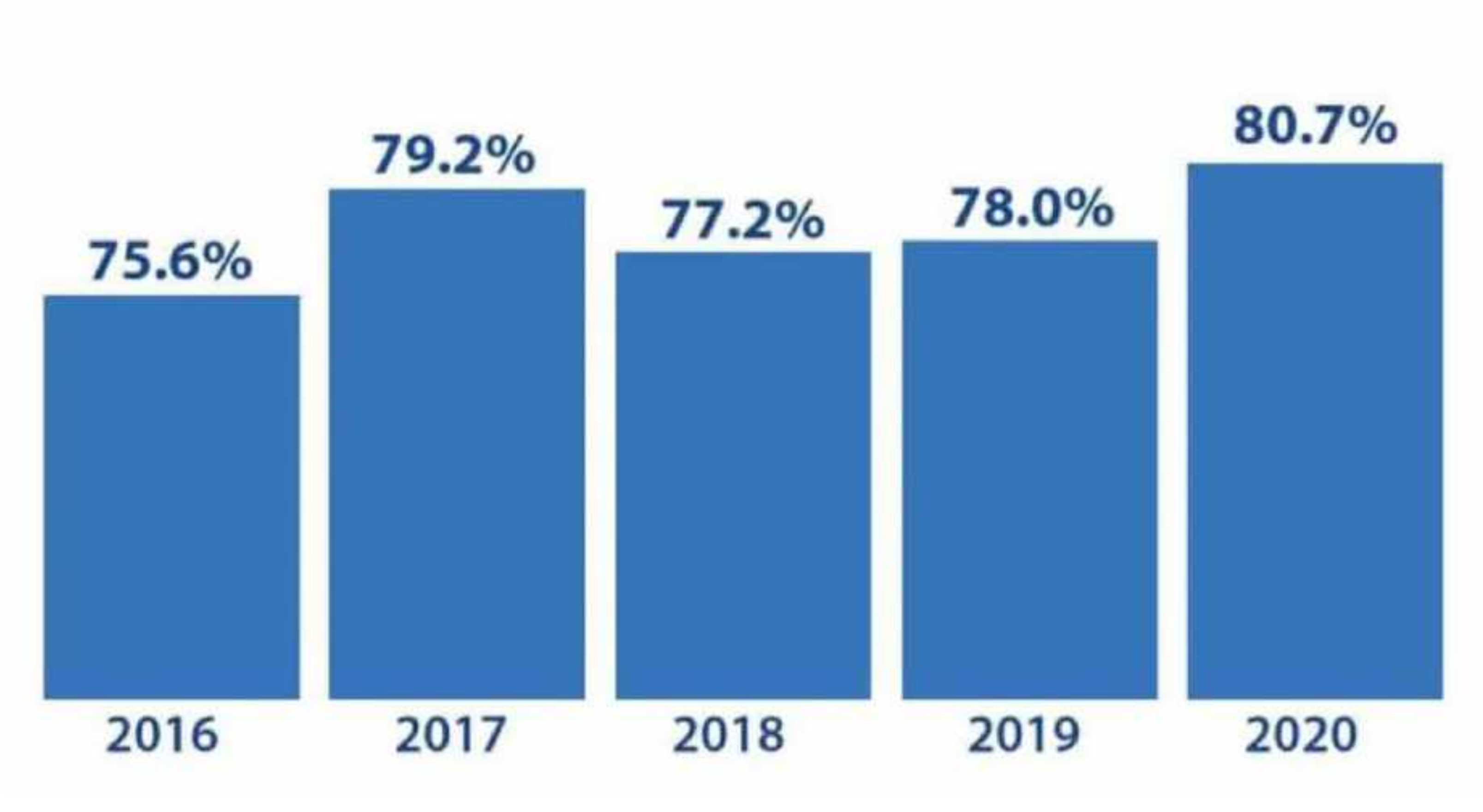
The cybercrime prediction stands, and over the past two-plus year
of major media outlets, academia, senior government officials, ass

Source: CyberCrime Magazine


TIME AND MONEY LOST TO CYBERCRIME
$114 BILLION
CYBERCRIME COST IN CASH IN 12 MONTHS
$274 BILLION
TOTAL LOSS OF TIME FOR VICTIMS IN 24 COUNTRIES OVER THE PAST 12 MONTHS
INDIA
15 Days/Victim
CASH COSTS
$4BN
TIME COSTS
$3.6BN
Extrapolated costs over the last 12 months – see methodology for more details. All figures are rounded

Source: CyberEdge 2020 Cyberthreat Defense Report

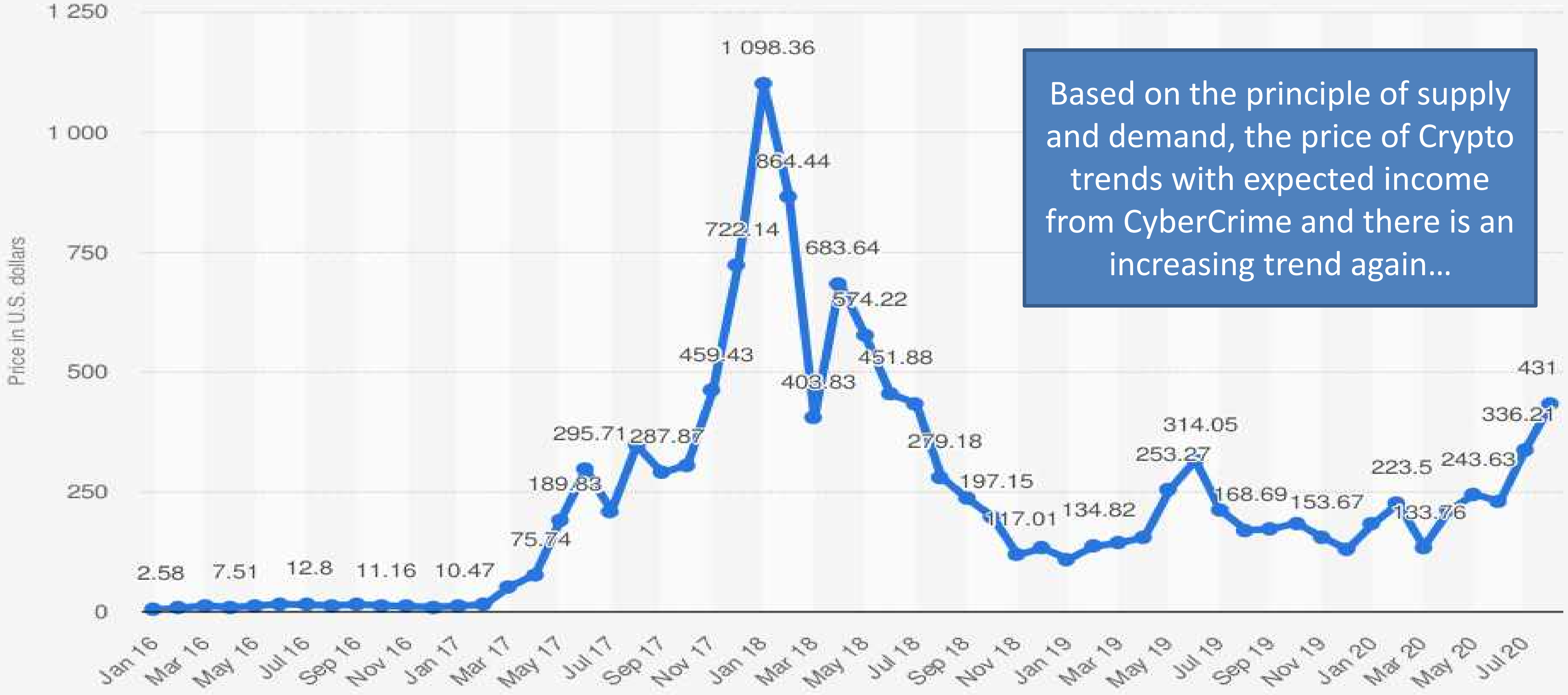
Companies Compromised at least Once



CyberEdge 2020 Cyberthreat Defense Report

Companies are being targeted and many more companies than ever are being hit. Compromise seems to be increasing per year and as we look at economic trends, tight economic years lead to increased cyber crime

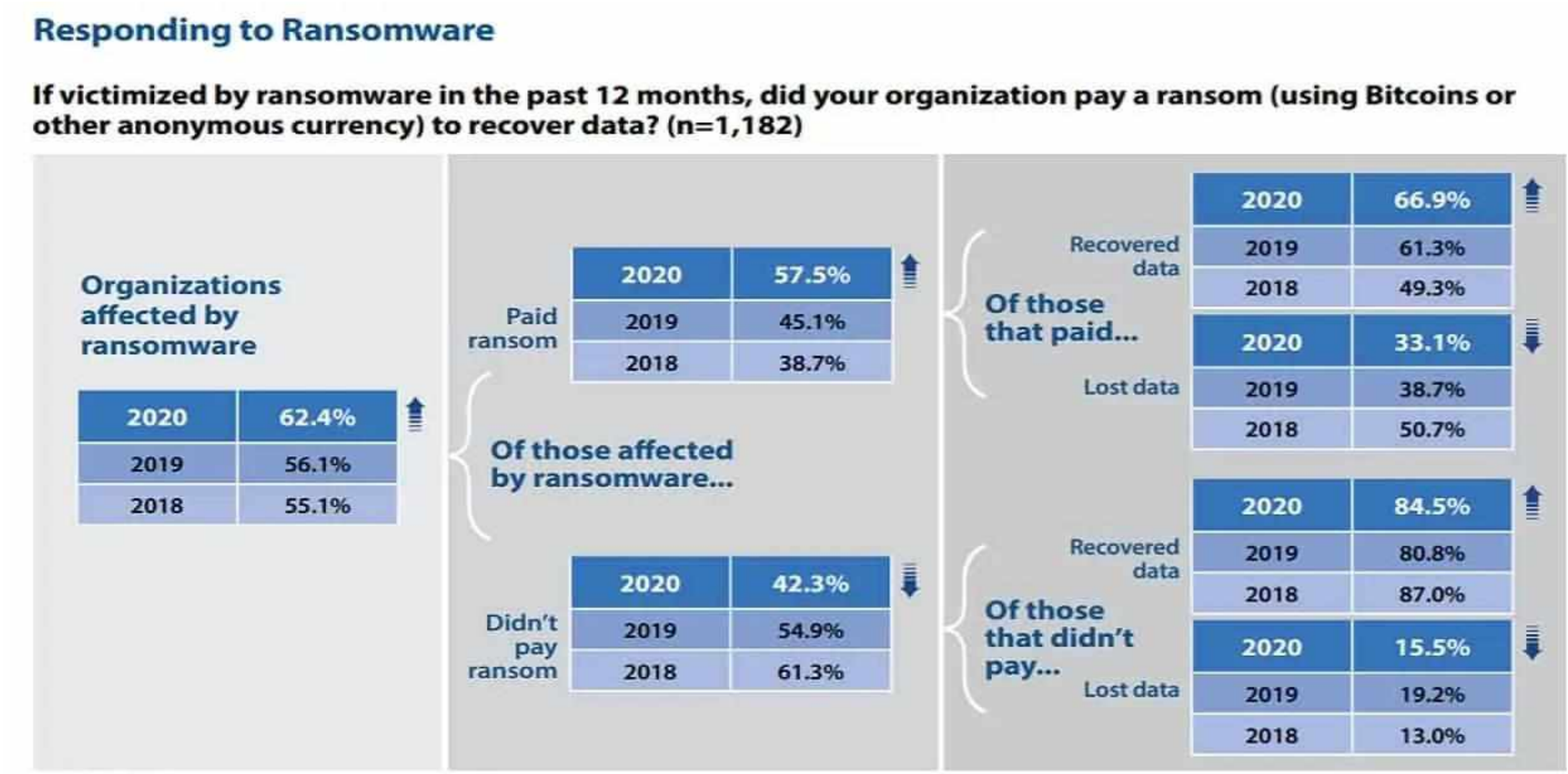
Price of Ethereum from January 2016 to August 2020 (in U.S. dollars)



Based on the principle of supply and demand, the price of Crypto trends with expected income from CyberCrime and there is an increasing trend again…

Source
CoinDesk
© Statista 2020

Additional Information:
Worldwide; CoinDesk; January 2016 to August 2020



Responding to Ransomware

If victimized by ransomware in the past 12 months, did your organization pay a ransom (using Bitcoins or other anonymous currency) to recover data? (n=1,182)

Organizations affected by ransomware

2020	62.4% ↑
2019	56.1%
2018	55.1%

Of those affected by ransomware...

Paid ransom

2020	57.5% ↑
2019	45.1%
2018	38.7%

Didn't pay ransom

2020	42.3% ↓
2019	54.9%
2018	61.3%

Of those that paid...

Recovered data

2020	66.9% ↑
2019	61.3%
2018	49.3%

Lost data

2020	33.1% ↓
2019	38.7%
2018	50.7%

Of those that didn't pay...

Recovered data

2020	84.5% ↑
2019	80.8%
2018	87.0%

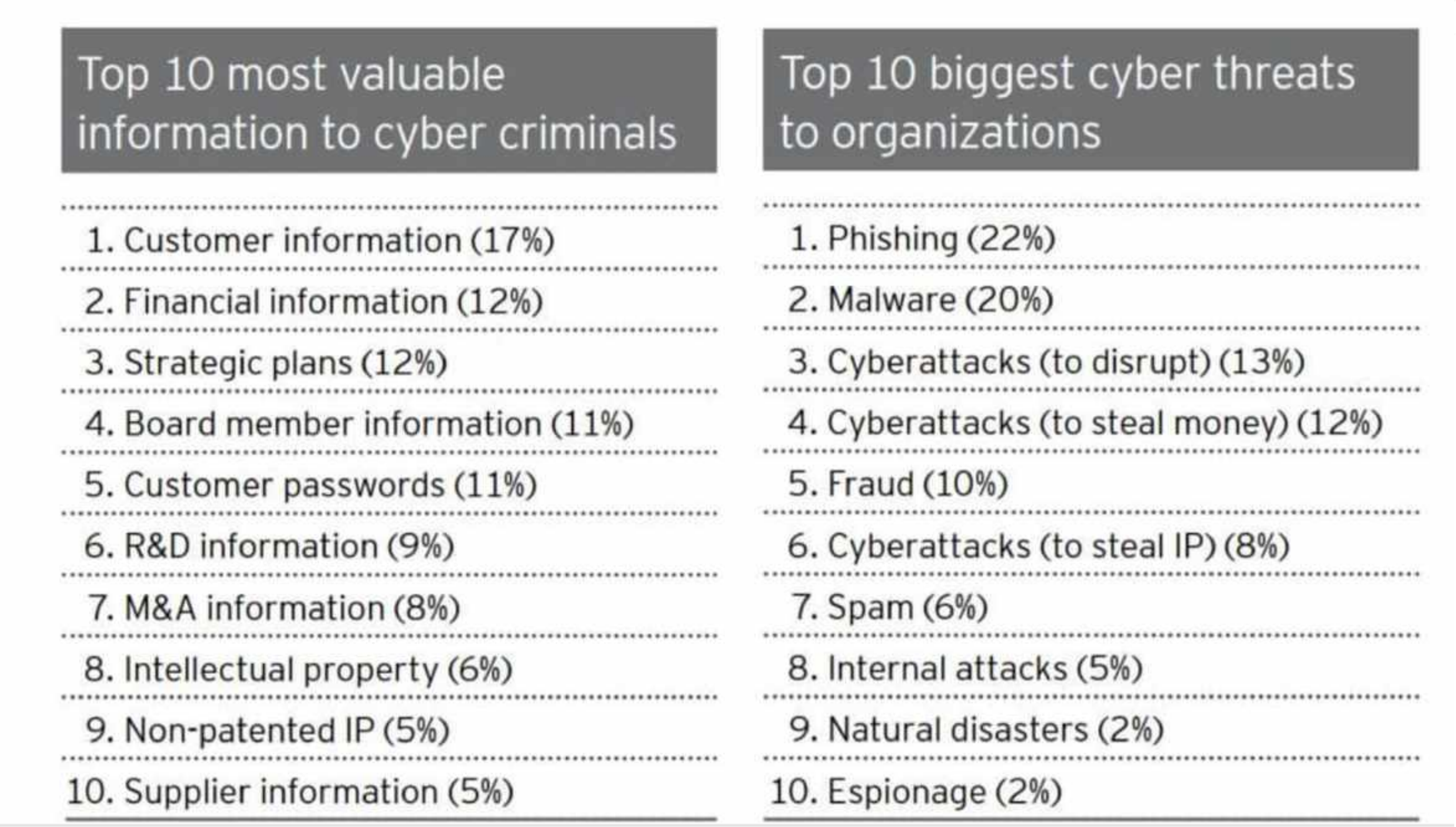
Lost data

2020	15.5% ↓
2019	19.2%
2018	13.0%

Source: Imperva 2020 Cyberthreat Defense Report

Busy?

ed



Top 10 most valuable information to cyber criminals	Top 10 biggest cyber threats to organizations
1. Customer information (17%)	1. Phishing (22%)
2. Financial information (12%)	2. Malware (20%)
3. Strategic plans (12%)	3. Cyberattacks (to disrupt) (13%)
4. Board member information (11%)	4. Cyberattacks (to steal money) (12%)
5. Customer passwords (11%)	5. Fraud (10%)
6. R&D information (9%)	6. Cyberattacks (to steal IP) (8%)
7. M&A information (8%)	7. Spam (6%)
8. Intellectual property (6%)	8. Internal attacks (5%)
9. Non-patented IP (5%)	9. Natural disasters (2%)
10. Supplier information (5%)	10. Espionage (2%)

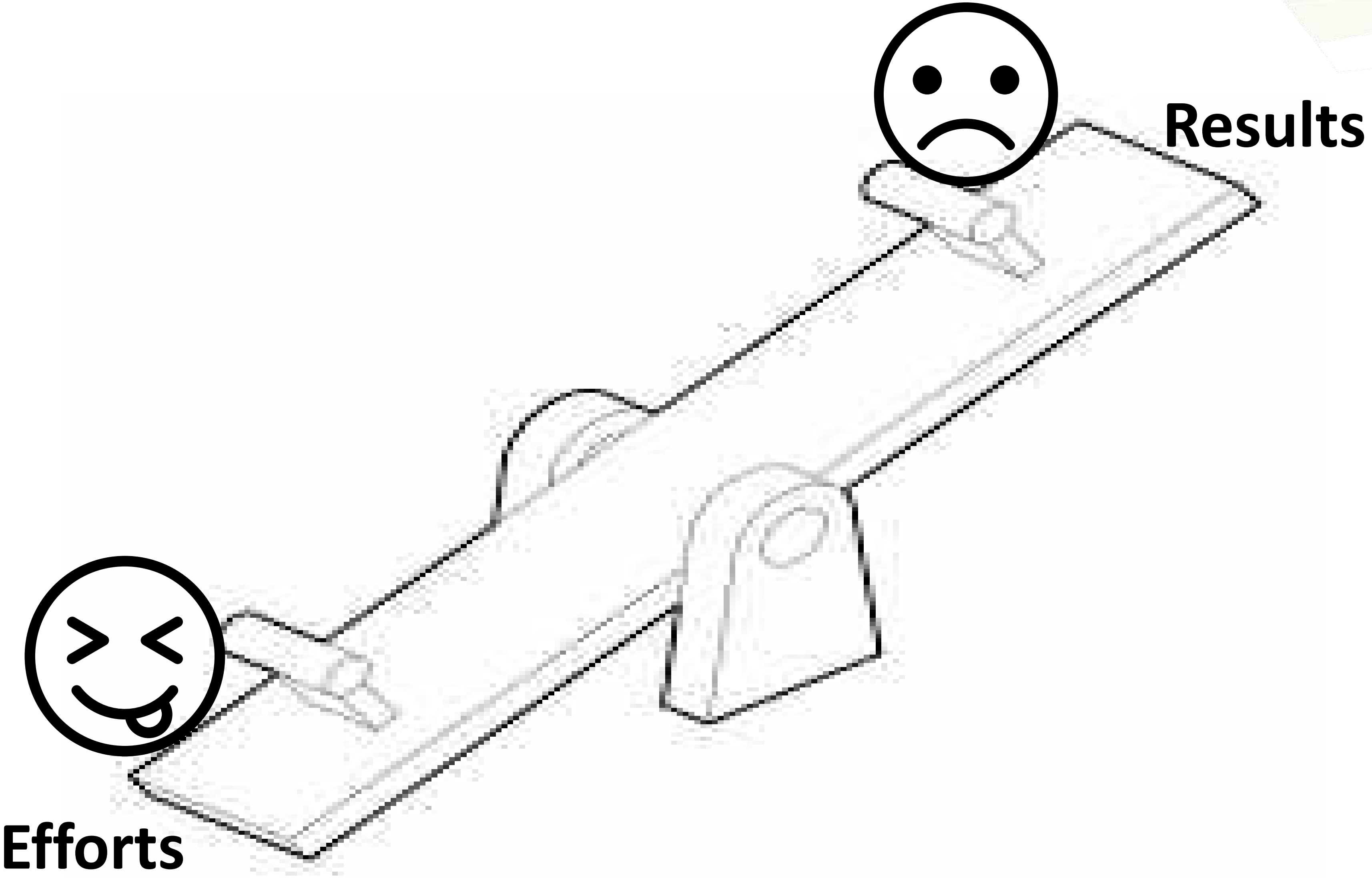
Source: EY (Global Information Security Survey 2018-2019)

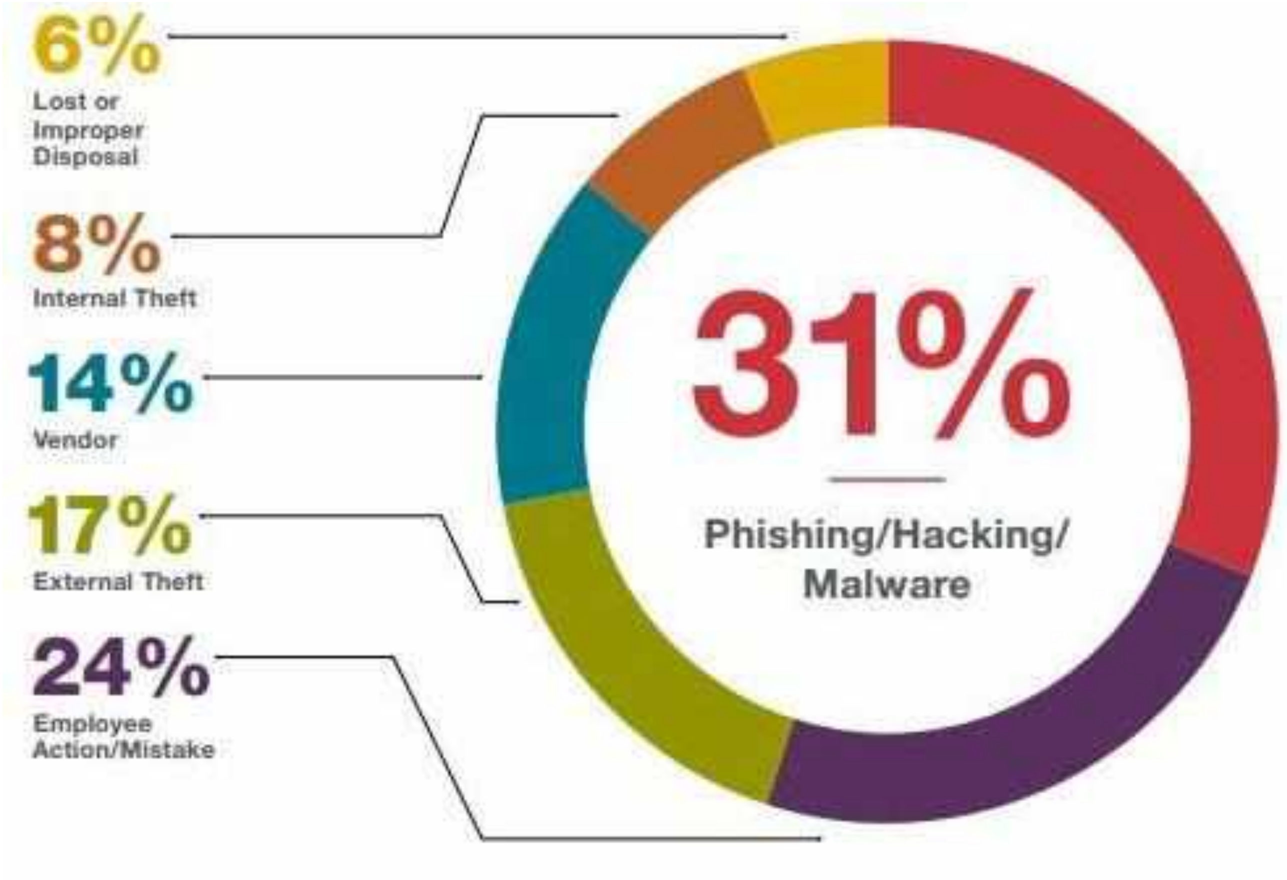
Busy!

3

The Foundations

Let us forget the Blame Game and Review the Major Causes of Breaches

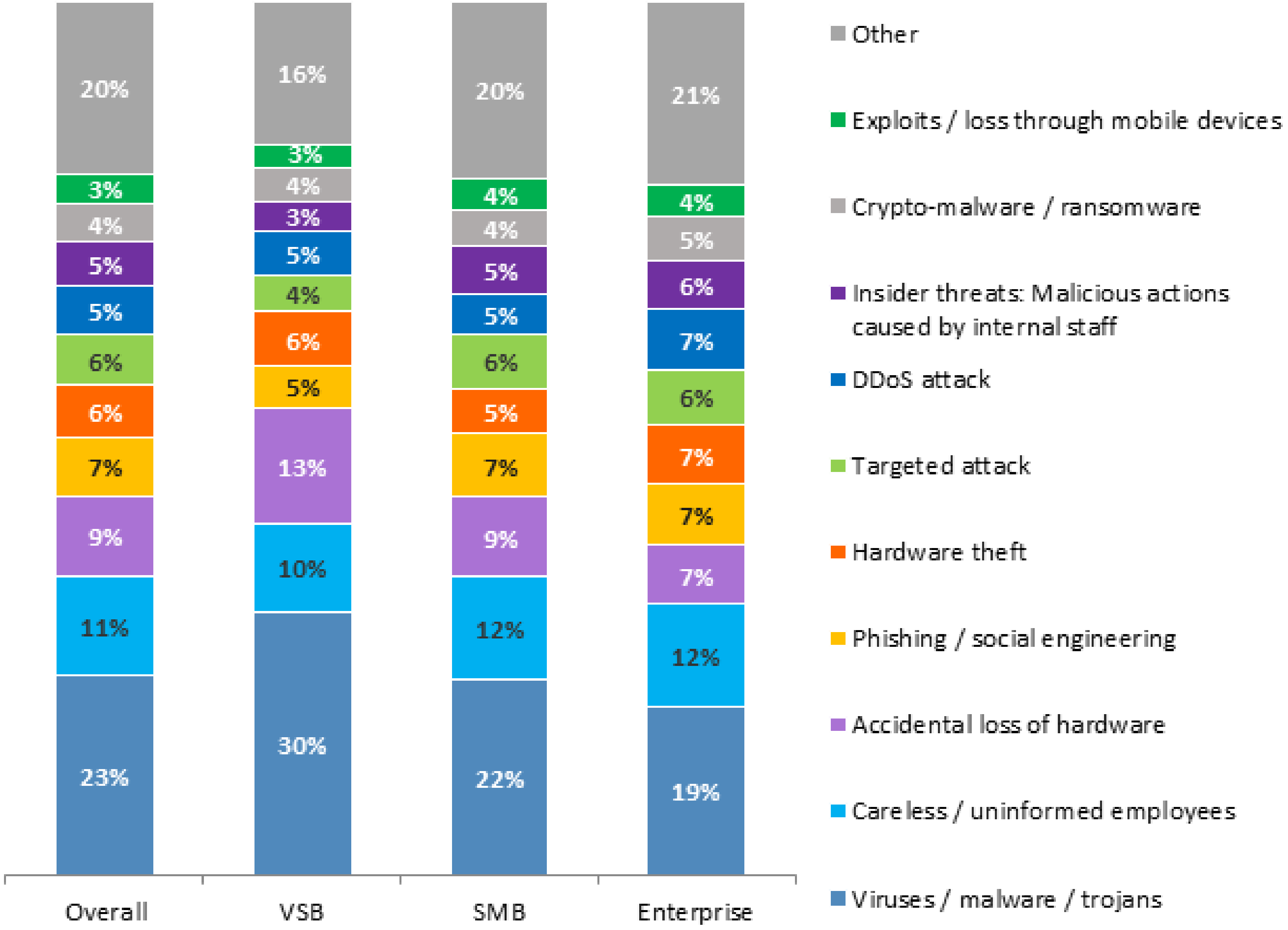

Results
Efforts



Attacks are mostly Internal in spite of various activities done to ensure the organization is protected, the easiest route for cyber attacks is through internal collaboration.

Leading Causes of Data Breaches/Cyber Threaats
Source: www.premierinsurancecorp.com

Many times, we spend much efforts on Technology and the Blame Game rather than solving the direct major company destroying factor – Breaches caused by failure to know what to do!



Sadly, lack of vigilance is the **Leading Cause of Breaches**

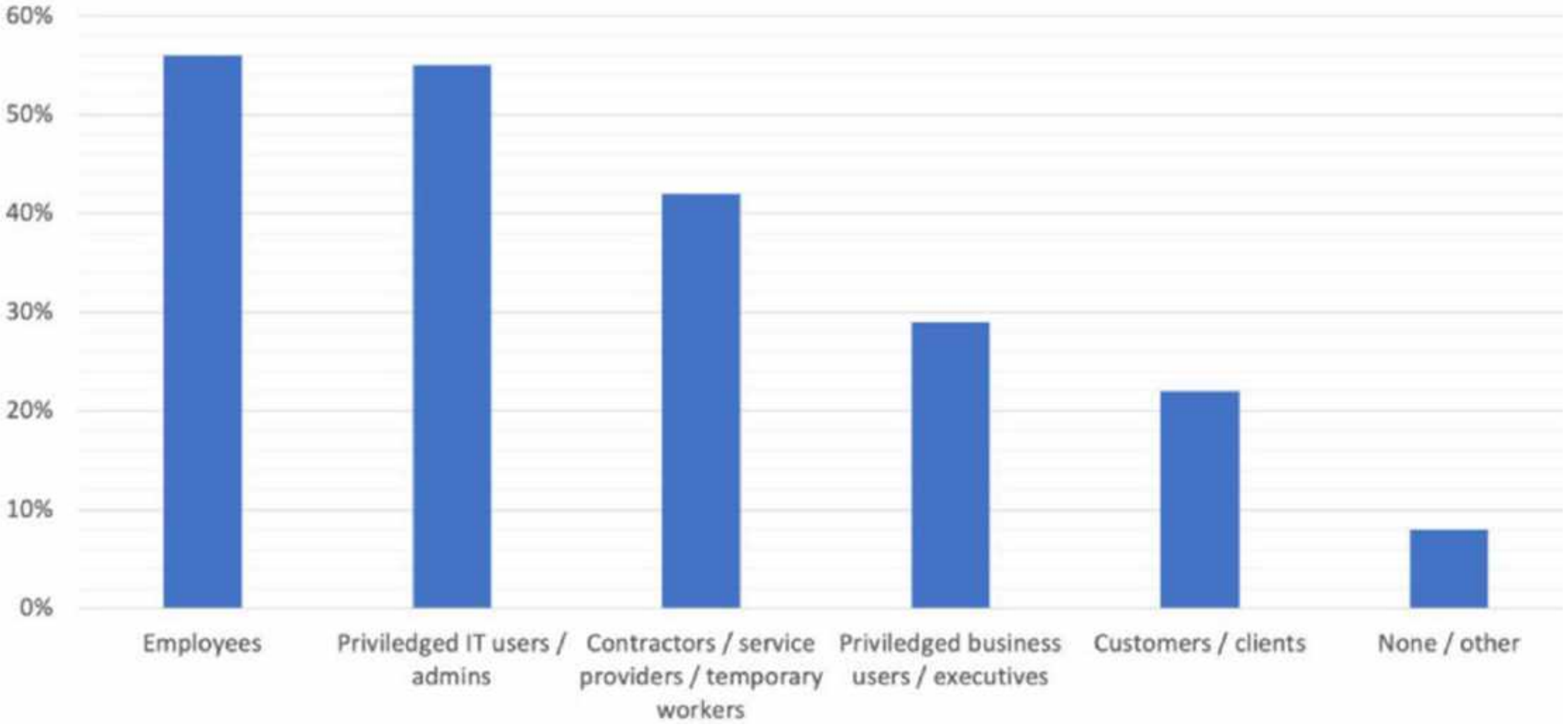
Cybercriminal tactics often leverage available information: **63 percent of network intrusions** are the result of **compromised user passwords and usernames**

Source: Microsoft

- **Phishing** is the number one type of threat action involved in data breaches. (Verizon's 2020 Data Breach Investigation Report)
- Microsoft reported a huge increase of 250% in phishing emails between January and December 2018, analyzing more than 470 billion email messages every month for this particular threat and for malware.
- CISCO states that (in its 2018 Annual Cybersecurity Report) 38% percent of malicious email attachments were Microsoft Office formats such as Word, Excel, PowerPoint
- **Archive files, the likes of .zip and .jar, represent around 37%** of all malicious file extensions Cisco observed, with malicious PDF files accounting for 14% of the total. *(Cisco)*
- **82% of cloud users have experienced security events caused by confusion** over who is responsible to secure the implementations *(Oracle and KPMG Cloud Threat Report 2019)*
- **35 percent of companies** were targeted by an SSL or TLS-based attack *(Gartner)*
- Fileless attacks were used in **77% of successful compromises in 2018** because they're increasingly effective at evading detection; as a consequence, the trend is bound to increase *(ENISA Threat Landscape Report 2018)*

What types of Insiders Cause the Greatest Compromise to our Organizations

Concentrating on these would reduce the risk to most organizations by over 60% and the only cost involved in the cost of creating more awareness



CSCS
RC 201018
CENTRAL SECURITIES CLEARING SYSTEM PLC

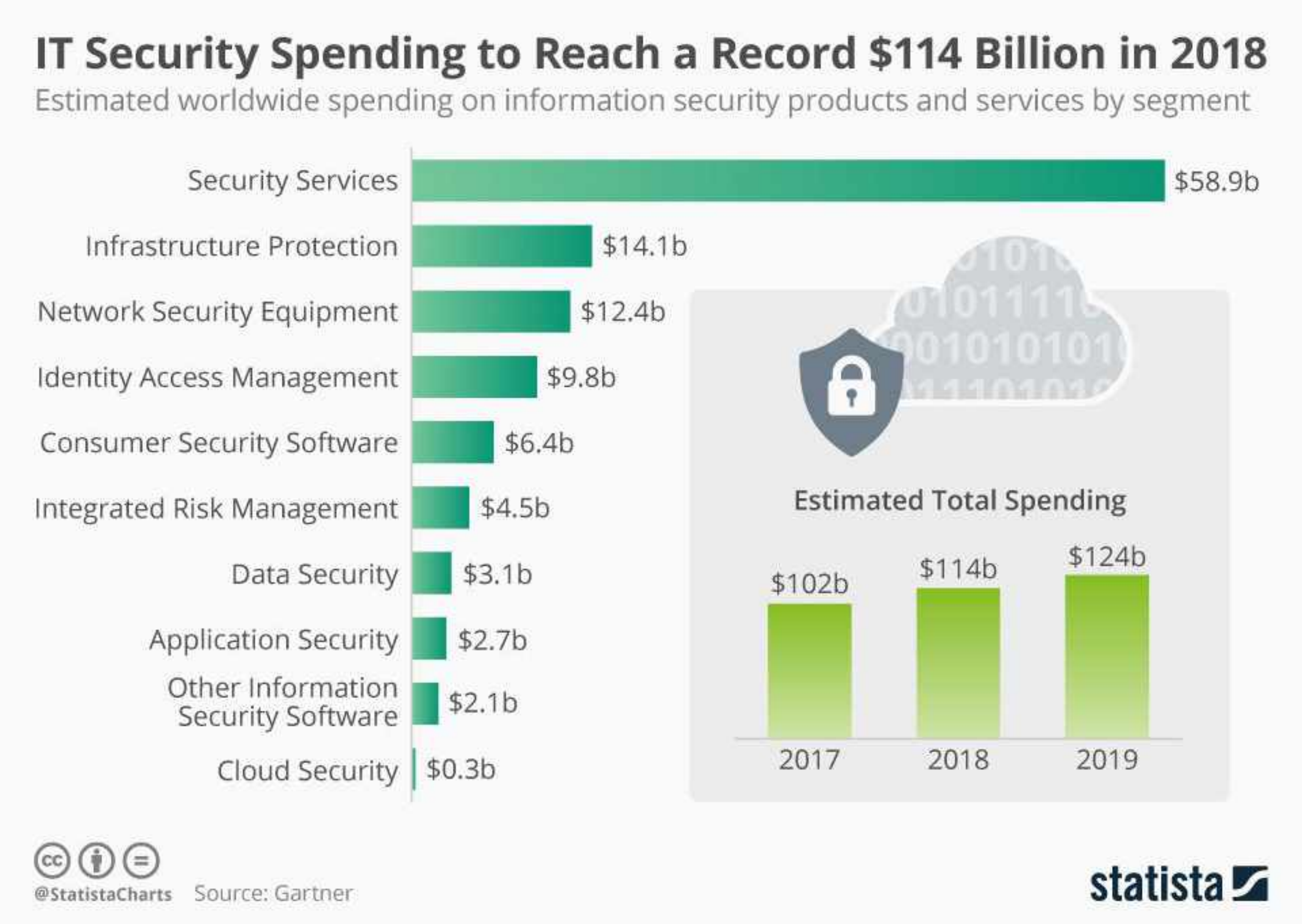
Security is the Work of Everyone!

d

4

The Fix

What can we do to ensure at a low cost, we cut off potential breaches



IT Security Spending to Reach a Record $114 Billion in 2018

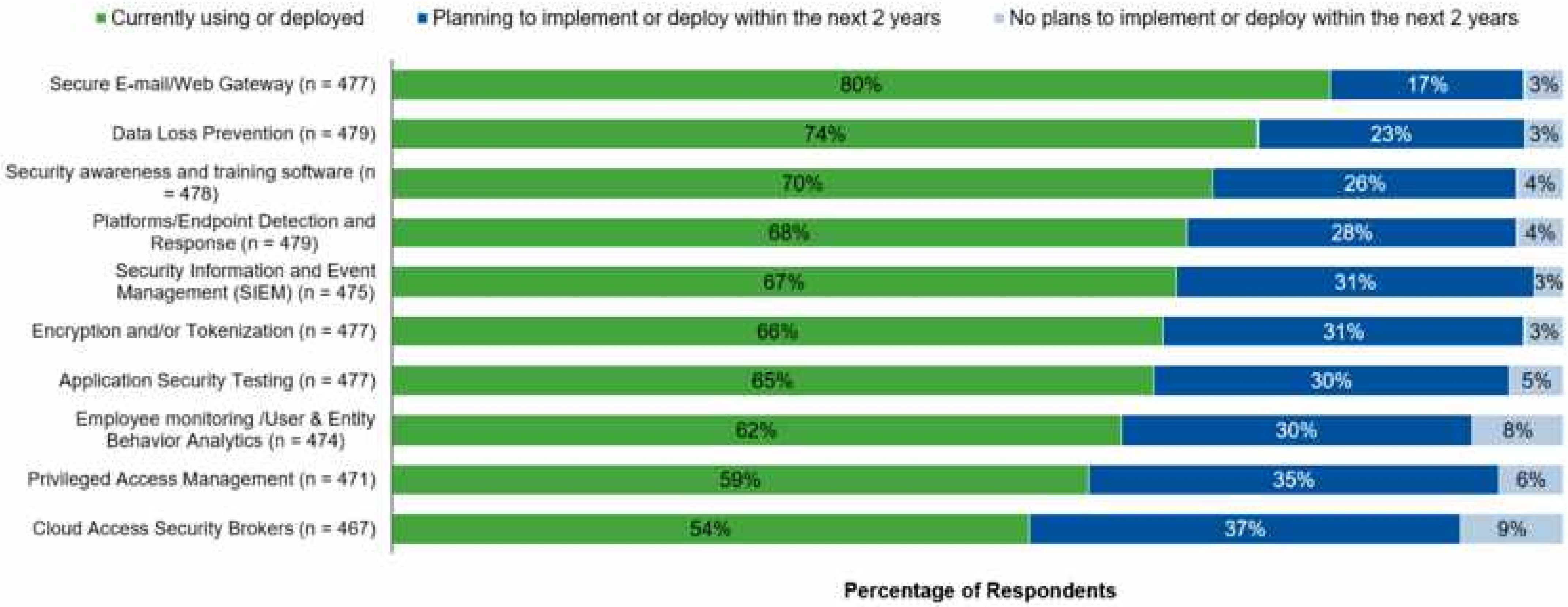
Estimated worldwide spending on information security products and services by segment

Source: Gartner

The pattern of spend on security show clearly that organizations are doing all they can to ensure they are more secured

Document Classification: CSCS Controlled

What are Global Firms spending on?



Base: All Respondents, excludes Not sure. N = As specified
Q. What phase of adoption is your organization currently in for the following technology products?

Gartner.

Sad Realities

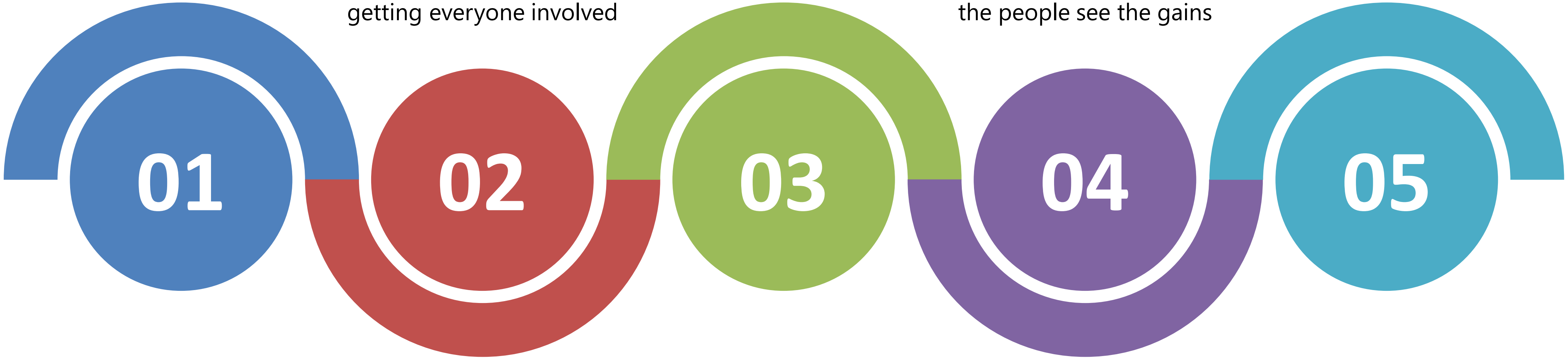
Source: Pwc, CyberCrimeMag, Infographics

- Only 61% of companies have a real budget for security awareness globally.
- 7 out of 10 companies have conducted phishing experiments to gauge employee preparedness but less than 1 continued with the training till the end
- 44% of companies surveyed are planning to spend more on security awareness
- 4 of top 5 security breaches are caused by negligence of people.
- PwC highlighted that 48% of businesses do not have an employee cyber security awareness training program

GIVE UP
KEEP GOING

How do we Achieve Better Awareness

Give the Specialists more opportunity to make
an impact in the organization



Make Security Viral

Security Awareness should be an integral part of the life of the company. Let it be a part of your DNA

Get People Involved

An organization is as strong as her weakest link. Make sure you are well secured by getting everyone involved

IT Security Guys are Normal

IT Security Specialists are not just GEEKs or PESSIMISTS. Engage them and let them be engaged

Be Positive Minded

Recraft the story and make it positive. Achieve more mileage by ensuring you let the people see the gains

Regular Engagements

Don’t stop. Just as the Cyber Criminals are looking for ways to hack and tag, ensure you are constantly improving.

How do we Achieve Better Awareness

Ensure it is an All-Encompassing Plan. Secure the following within the Enterprise!

People

Ensure people are properly trained and made aware of the impact of not putting the policies in place within the organization. Let your people be knowledgeable and committed

Policies

Ensure you put in place policies that will create the awareness and control user behaviour

Processes

Review all processes and ensure that all loopholes are properly plugged. Remove vulnerabilities as fast as you can

Technology

Deploy Technology platforms that will protect your organization. Make proper monitoring and where possible leverage on external help

Recommended CyberSecurity Skills Matrix

The Board

Inspire positive and deliberate actions towards increasing Cybersecurity. Achieve this through the Assurance Functions

Executive Management

Drive decisions that will protect the organization and support capacity development for cybersecurity.

Supervisors

Ensure every team is secured. Create proper processes and safe-guard the organization

Senior Management

Lead the initiatives and ensure all departments have the right awareness and commitment

Team Members

Be knowledgeable, comply with all instructions and importantly ensure you report any exceptions

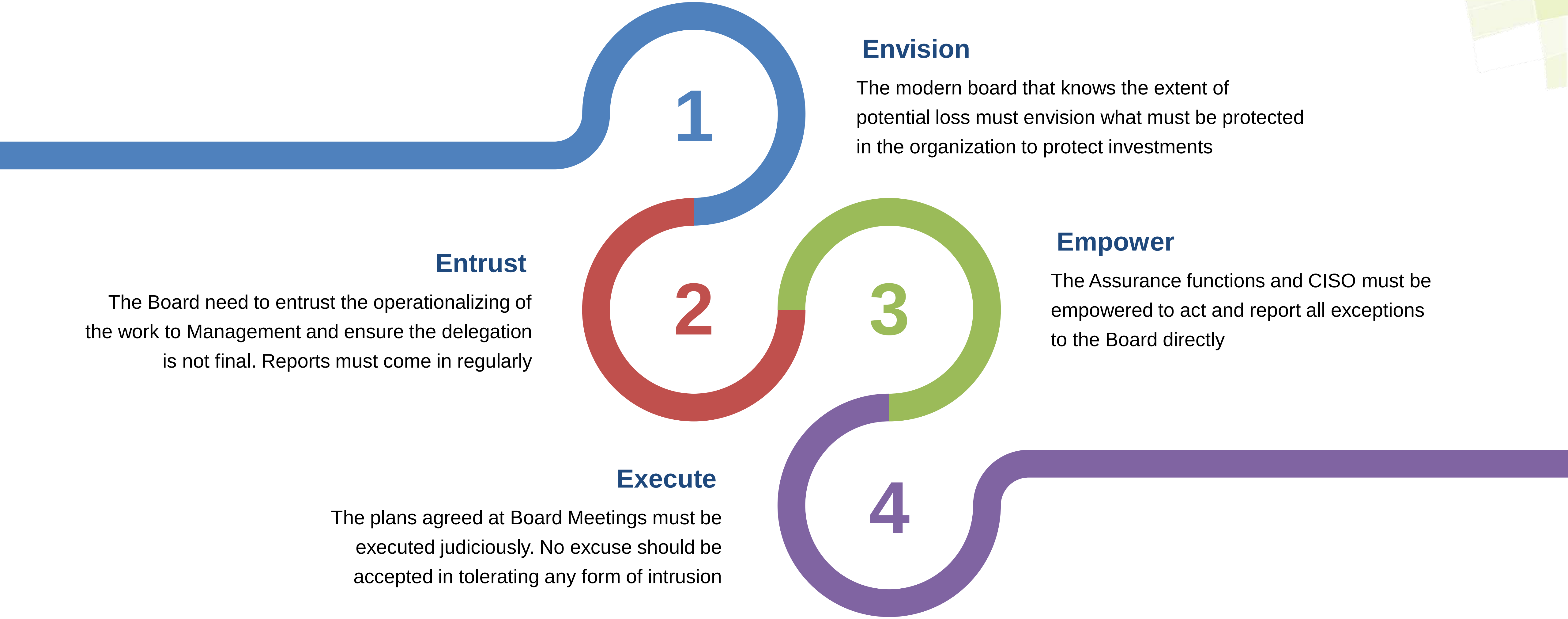
Partners & Stakeholders

Ensure you do not create the weakest link in cybersecurity of the organization.

CSCS
RC 201018
CENTRAL SECURITIES CLEARING SYSTEM PLC

How to Achieve CyberSecurity Excellence

Board



Envision

The modern board that knows the extent of potential loss must envision what must be protected in the organization to protect investments

Entrust

The Board need to entrust the operationalizing of the work to Management and ensure the delegation is not final. Reports must come in regularly

Empower

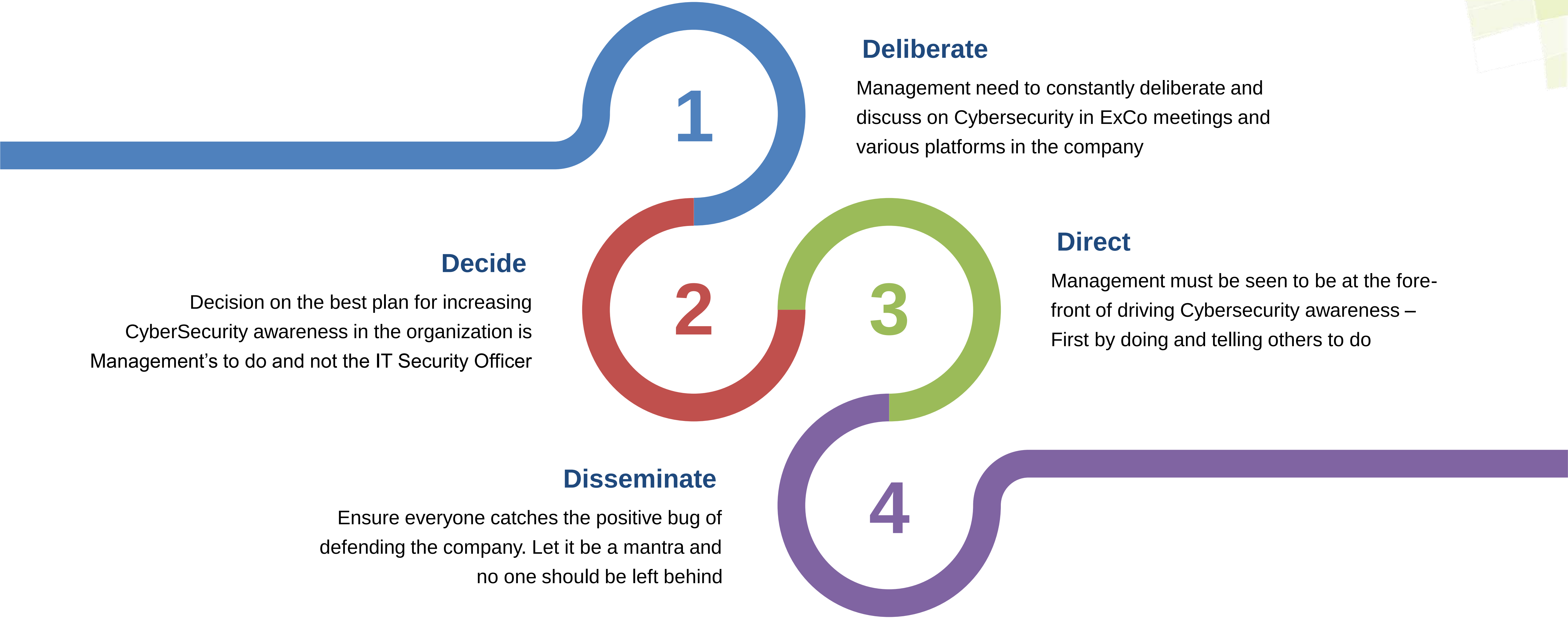
The Assurance functions and CISO must be empowered to act and report all exceptions to the Board directly

Execute

The plans agreed at Board Meetings must be executed judiciously. No excuse should be accepted in tolerating any form of intrusion

How to Achieve CyberSecurity Excellence

Management



Deliberate

Management need to constantly deliberate and discuss on Cybersecurity in ExCo meetings and various platforms in the company

Decide

Decision on the best plan for increasing CyberSecurity awareness in the organization is Management’s to do and not the IT Security Officer

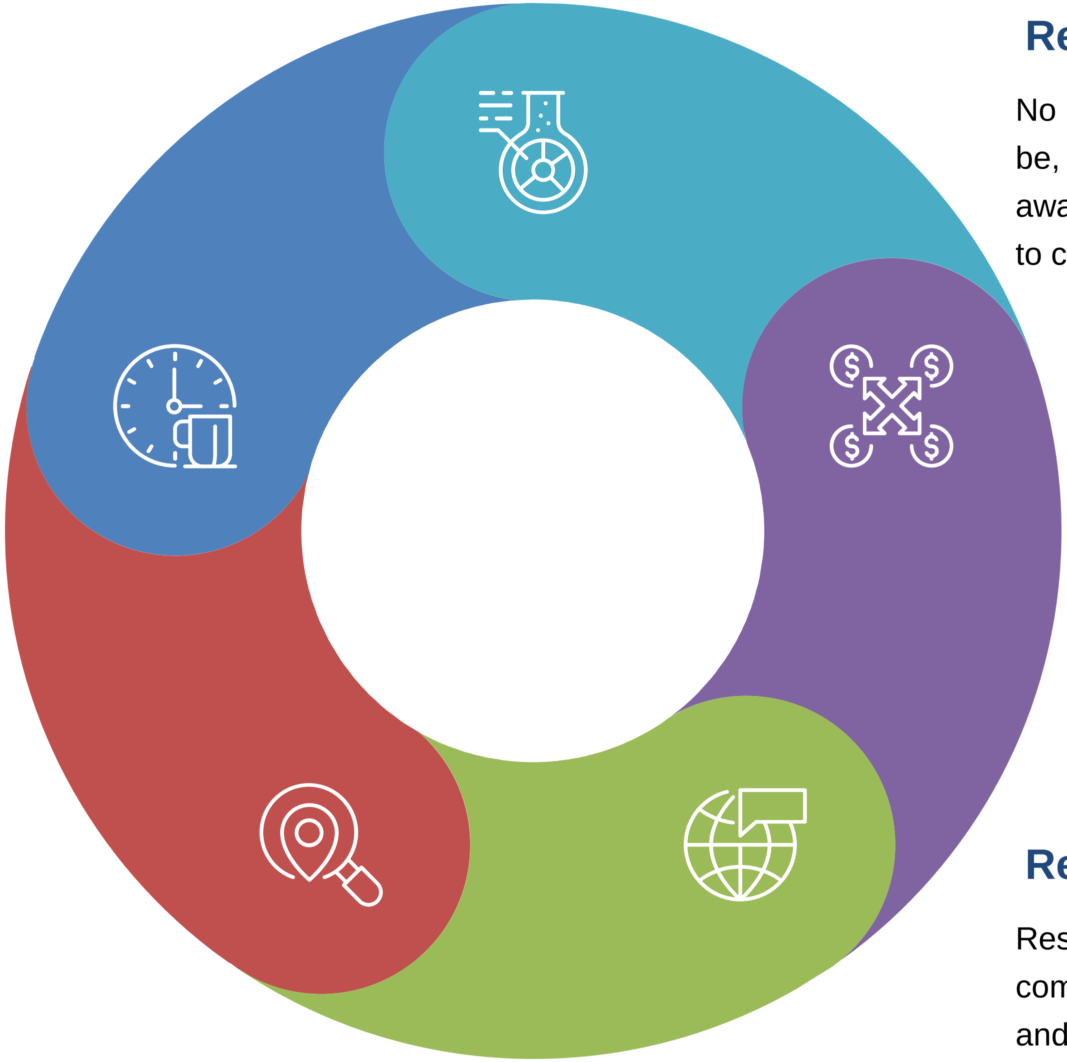
Direct

Management must be seen to be at the fore-front of driving Cybersecurity awareness – First by doing and telling others to do

Disseminate

Ensure everyone catches the positive bug of defending the company. Let it be a mantra and no one should be left behind

How to Measure Success



Readiness

No matter how tough an organization might be, a true test of proper cybersecurity awareness is the ability of the organization to come back after any attack

Resilience

How resilient the organization is when attacks happen is critical. When tests are done, how many people click the link for example?

Restoration

Restoration of the profit margins of the company as a result of savings from time and money spent when attacks happen

Reputation

Improvement in the reputation of the company as an organization where cyber attacks hardly succeed

Reduction

Reduction in number of successful cyber attacks is a major way of measuring the success

5

Finally…

… Make it FUN, but make it REAL

if you
SEE
something
SAY
something™

U.S. DEPARTMENT OF HOMELAND SECURITY

RC 201018

CENTRAL SECURITIES CLEARING SYSTEM PLC

Thank You for Listening. See you SAFE …………………………

ed

Thank You

Join the next CSCS Webinar Series