Barbarians at the Gate

Cybersecurity for Business Survival

SWARMNETICS

More than 20 years and 25 cities

First 8 years

- Software development
- Network operations
- Incident response
- Security management
- IT internal audit

Next 9 years

- Sarbanes Oxley 404 consulting
- PCI DSS assessment
- Security and IT audits
- Technology risk management
- Cybersecurity consulting

Last 4 years …

SWARMNETICS

Ethical hacking services built on bug bounty model

swarmnetics.com

Data Privacy Asia

Conference for data protection, privacy and cybersecurity leaders

dataprivacyasia.com

CPO MAGAZINE

Online publication for data protection, privacy and cybersecurity pros

cpomagazine.com

Objective:

Get a working knowledge of cyber risks and controls

Evolving Cyber Threat Landscape

Understand how digitalization has led to growth of the both the economy and cybercrime

You Have Either Been Hacked or Will Be

Learn more about cyber threats and the prevalent attacks

Keeping the Barbarians Outside the Gate

Discuss an effective approach to cyber defense

My Tech Is Better Than Your Tech

Take a look at the future of cyber defense

Evolving Cyber Threat Landscape

SWARMNETICS

Rise of the digital economy

Digitalization to produce

US$100 trillion

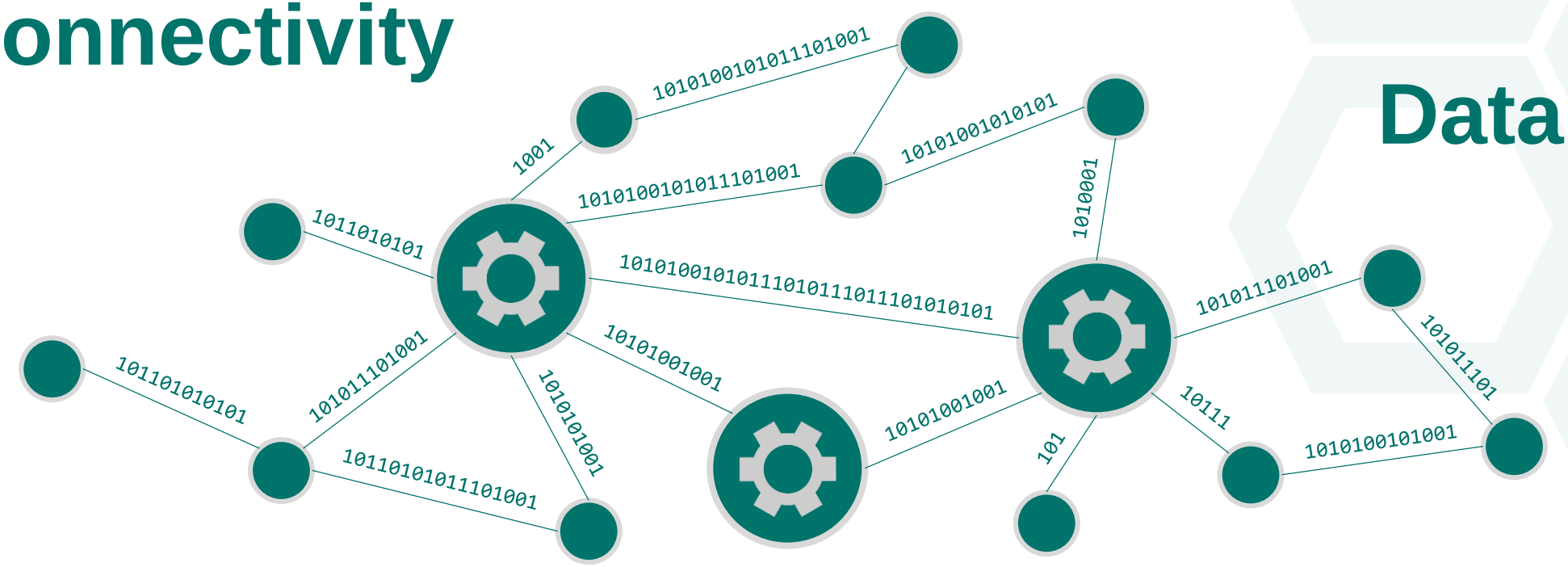
in value by 2025.

https://www.weforum.org/press/2016/01/100-trillion-by-2025-the-digital-dividend-for-society-and-business/

Accelerated by growth in …

Connectivity

Data

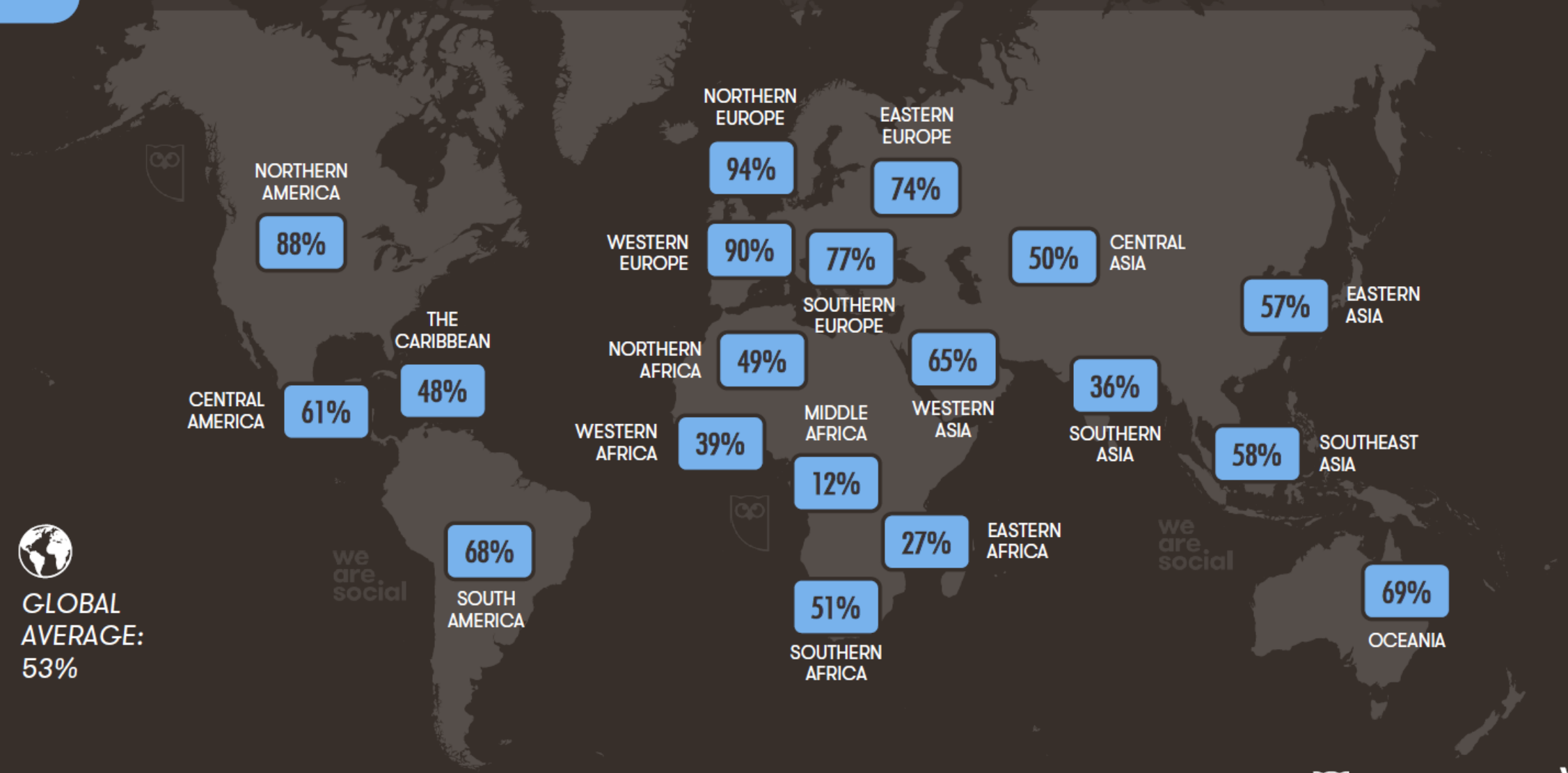


Technology

JAN 2018

INTERNET PENETRATION BY REGION

REGIONAL PENETRATION FIGURES, COMPARING INTERNET USERS TO TOTAL POPULATION



SOURCES: INTERNETWORLDSTATS; ITU; EUROSTAT; INTERNETLIVESTATS; CIA WORLD FACTBOOK; MIDEASTMEDIA.ORG; FACEBOOK; GOVERNMENT OFFICIALS; REGULATORY AUTHORITIES; REPUTABLE MEDIA. **NOTE:** PENETRATION FIGURES ARE FOR TOTAL POPULATION, REGARDLESS OF AGE.

JAN 2018

INTERNET USE

BASED ON ACTIVE INTERNET USER DATA, AND ACTIVE USE OF INTERNET-POWERED MOBILE SERVICES

TOTAL NUMBER OF ACTIVE INTERNET USERS

4.021

BILLION

INTERNET USERS AS A PERCENTAGE OF THE TOTAL POPULATION

53%

TOTAL NUMBER OF ACTIVE MOBILE INTERNET USERS

3.722

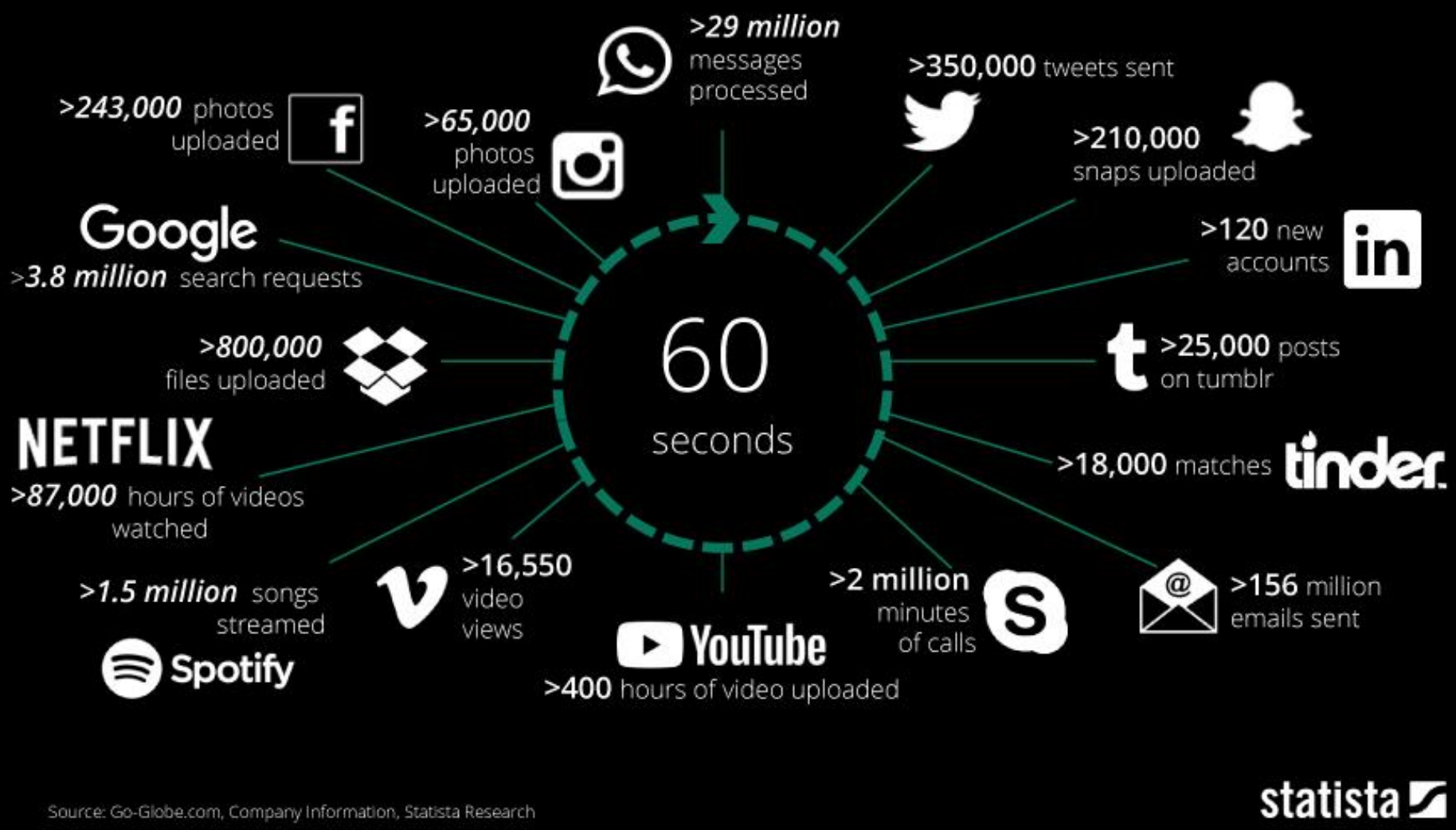
BILLION

MOBILE INTERNET USERS AS A PERCENTAGE OF THE TOTAL POPULATION

49%

SOURCES: INTERNETWORLDSTATS; ITU; EUROSTAT; INTERNETLIVESTATS; CIA WORLD FACTBOOK; MIDEASTMEDIA.ORG; FACEBOOK; GOVERNMENT OFFICIALS; REGULATORY AUTHORITIES; REPUTABLE MEDIA.. **NOTES:** PENETRATION FIGURES ARE FOR FULL POPULATION, REGARDLESS OF AGE.

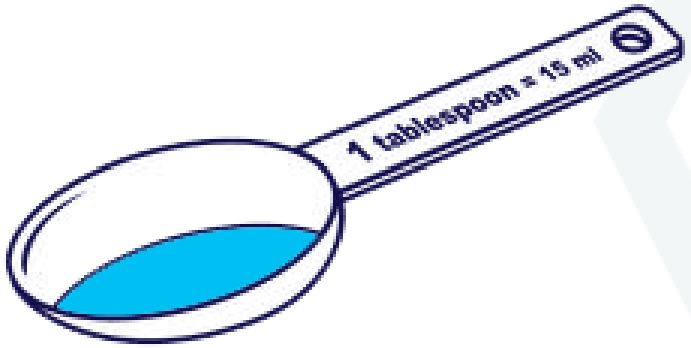
One minute on the Internet in 2017



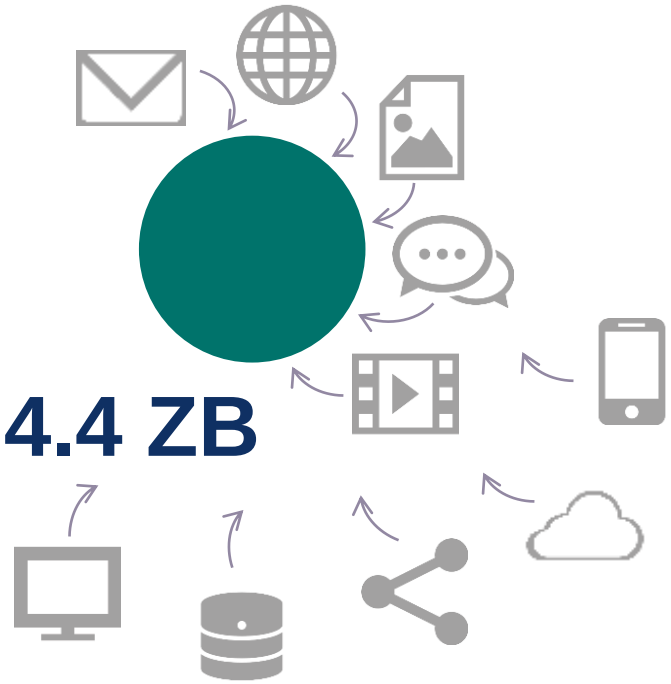
180,000,000,000,000,000,000,000

180 zettabytes by 2025

1 byte =



User Generated Content



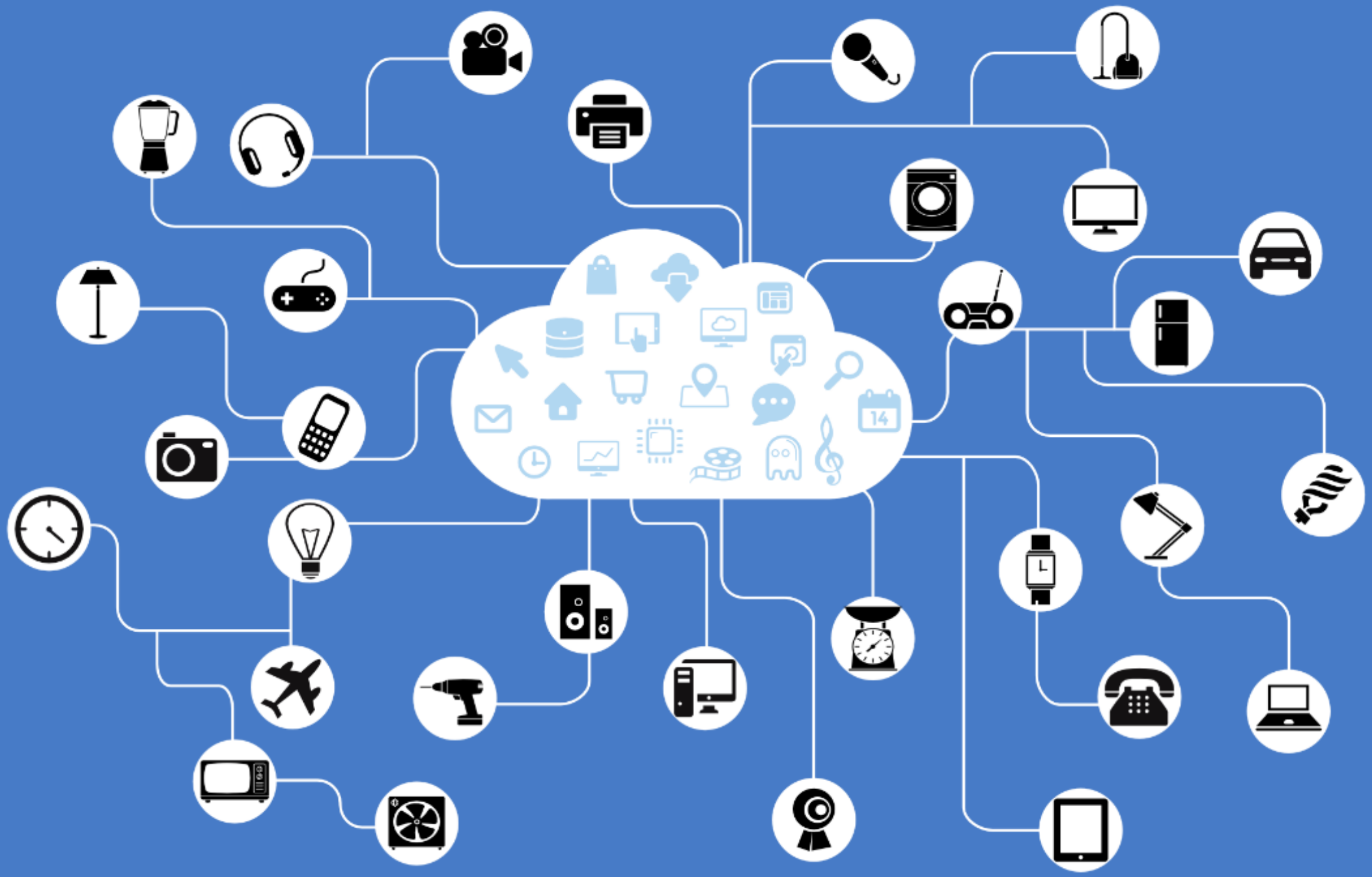
4.4 ZB

180 ZB

2013

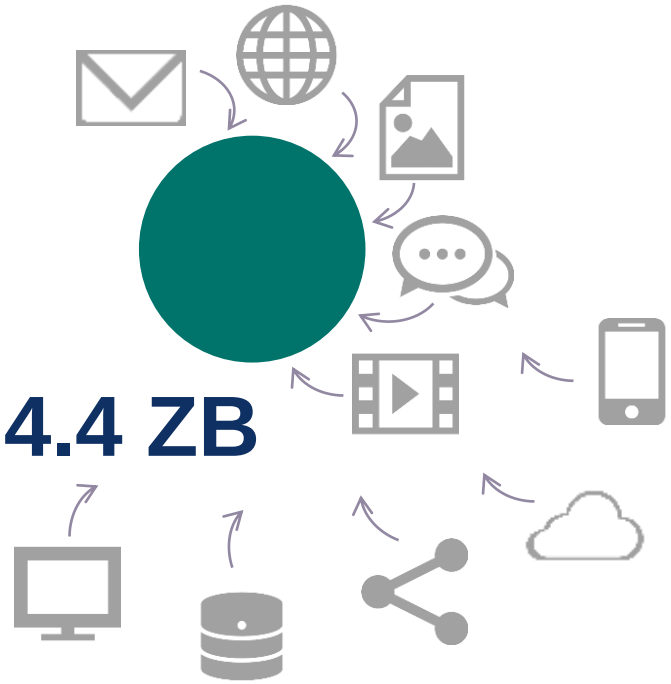
2025

100 GB/h




Analogue
World
⬇
Digital
Personal
Data

User Generated Content



4.4 ZB

Machine Generated Content

Location Data

Measurement Data

Status Data

180 ZB

80 billion connected devices by 2025

2013 → **2025**

Active → Passive Generators

Smart city investments – US$135 billion by 2021

- Data hungry – Convert analogue world to digital data
- Enabled by Internet of Things (IoT), data analytics, artificial intelligence, surveillance tech
- Smart metering, smart cameras, facial recognition, video/audio analytics, environmental monitoring

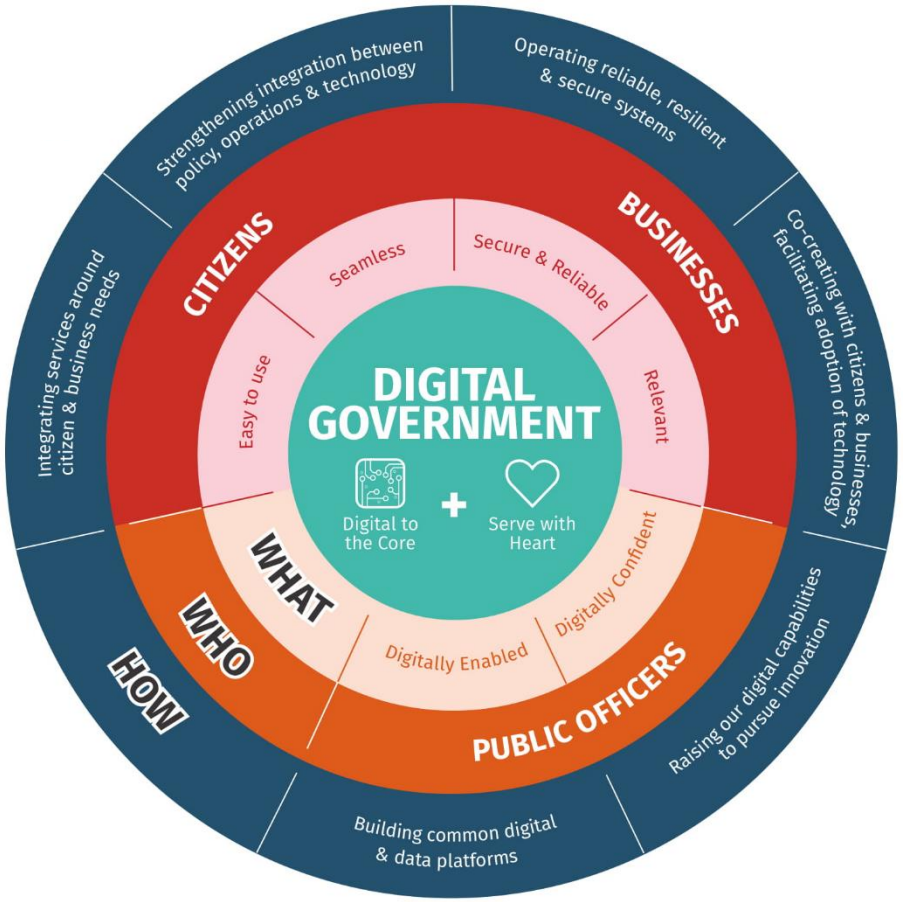
https://www.idc.com/getdoc.jsp?containerId=prUS43576718

Countries push for eGovernment

90 offer single entry portals on public information and/or online services

128 provide data sets on government spending in machine readable formats

148 provide at least one form of online transactional services.



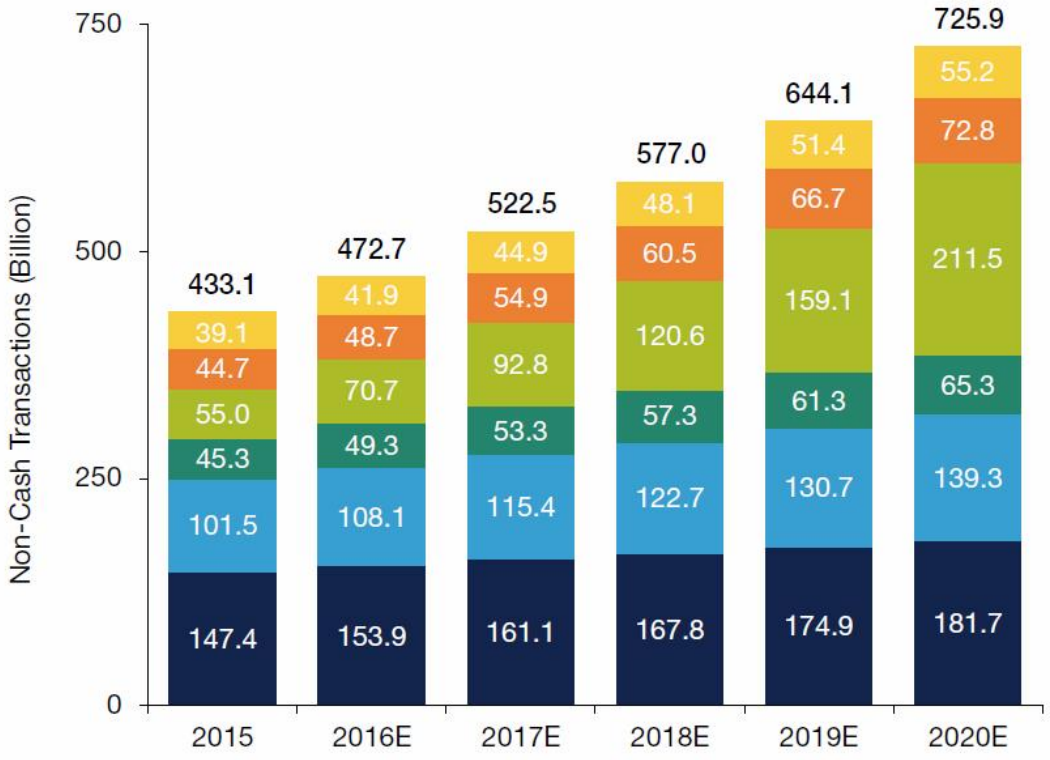
https://publicadministration.un.org/egovkb/en-us/reports/un-e-government-survey-2016
https://www.tech.gov.sg/Digital-Government-Transformation/Digital-Government-Blueprint

Digital banking users to reach 2 billion in 2018, representing nearly 40% of global adult population

https://www.juniperresearch.com/press/press-releases/digital-banking-users-to-reach-2-billion

Electronic payments continue to grow rapidly

Figure 2.1 Number of Worldwide Non-Cash Transactions (Billion), by Region, 2015–2020E



	CAGR ('15 –'20E)	Growth ('15 –'16E)	
Global	**10.9%**	**9.1%**	
Latin America	7.1%	7.2%	Developing 19.6%
CEMEA	10.2%	8.9%	
Emerging Asia	30.9%	28.6%	
Mature Asia-Pacific	7.6%	8.8%	Mature 5.6%
Europe (including Eurozone)	6.5%	6.5%	
North America	4.3%	4.4%	

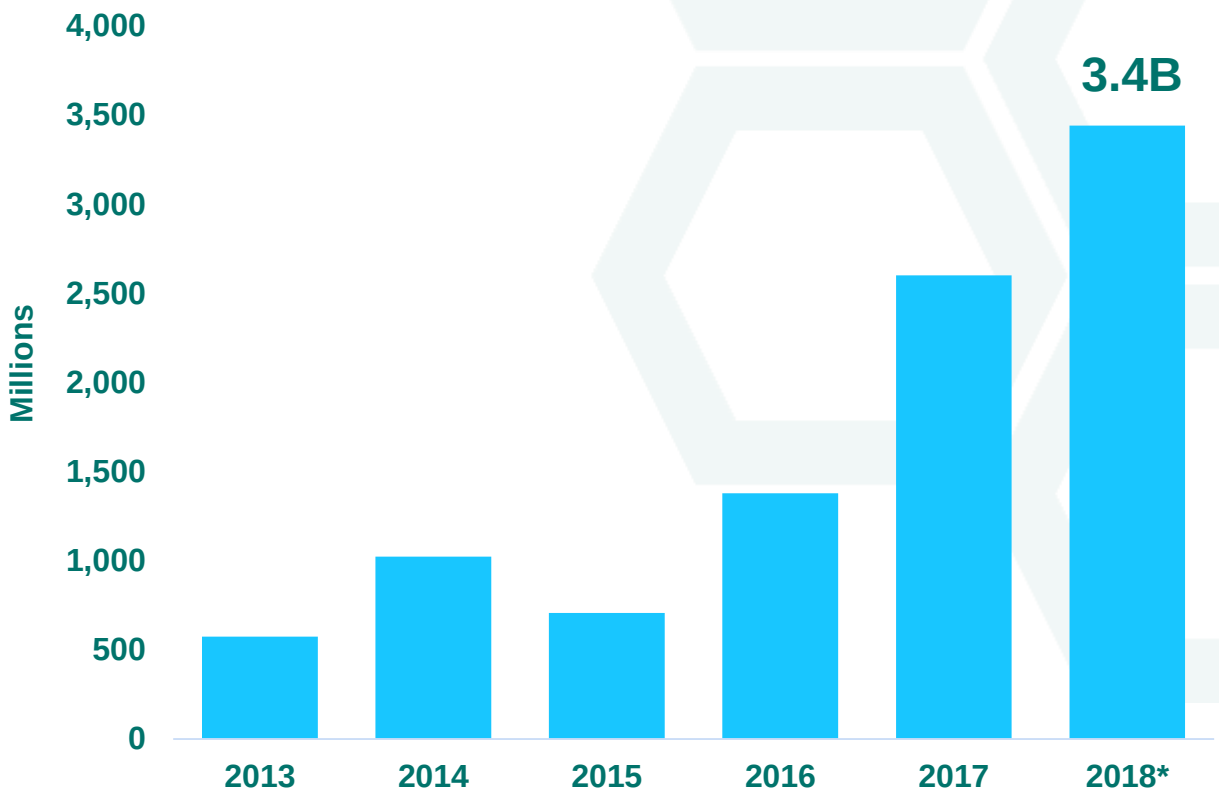
https://www.worldpaymentsreport.com/reports/noncash

Cyberattacks:
Top 10 global risks for doing business

Cybercrime:
Cost to hit US$8 trillion over the next five years

http://reports.weforum.org/global-risks-2018/global-risks-2018-fractures-fears-and-failures/

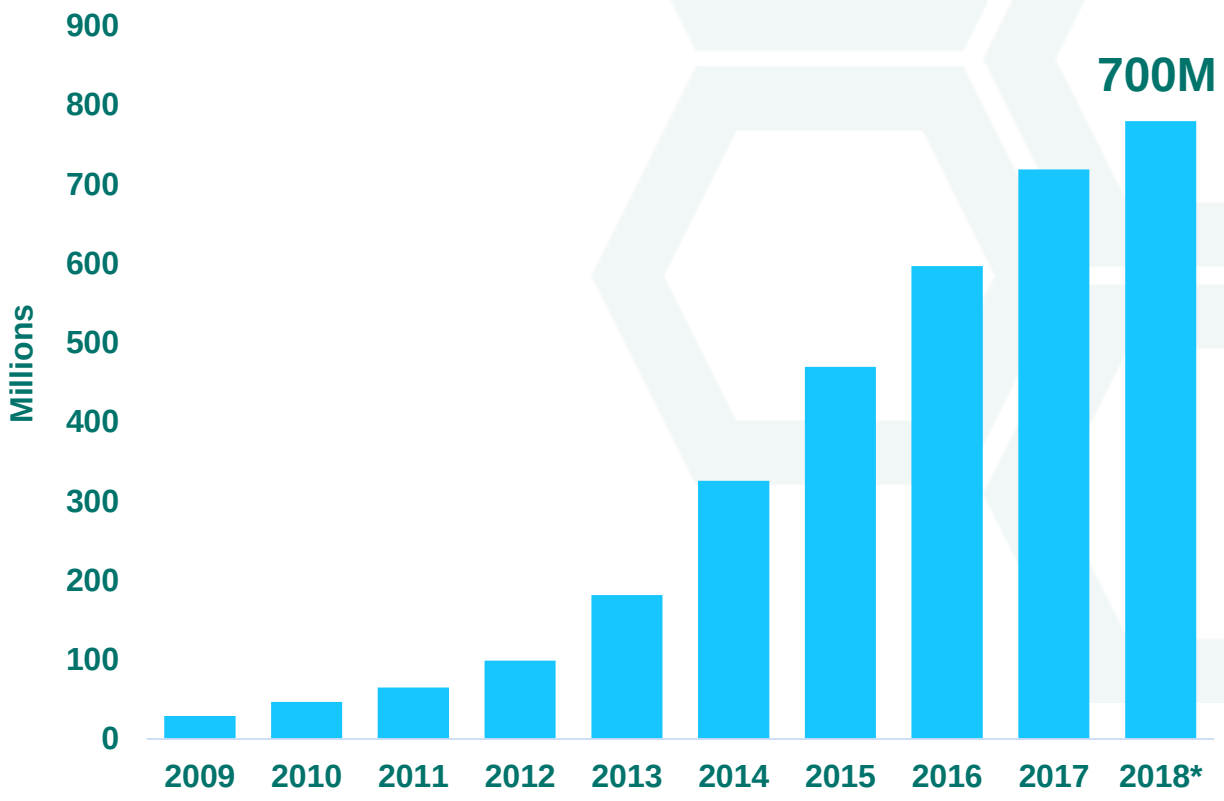
More than 9 billion data records lost or stolen since 2013



** As of July 2018*

https://breachlevelindex.com/

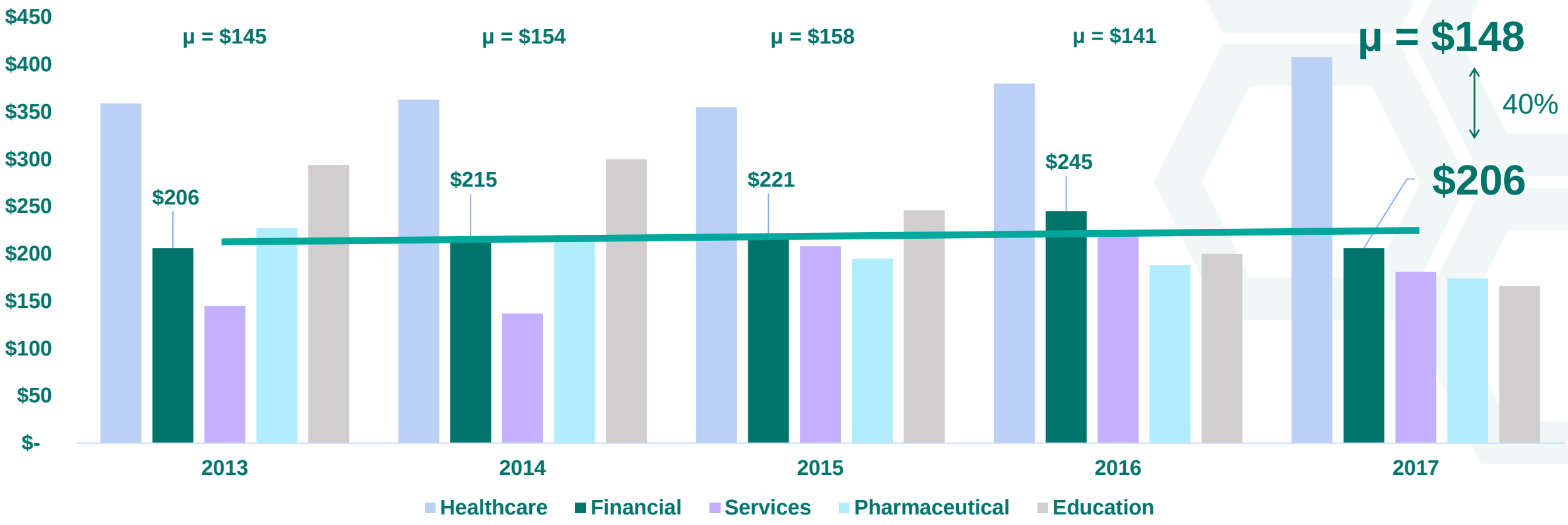
More than 700 million malware in 2017



** As of July 2018*

https://www.av-test.org/en/statistics/malware/

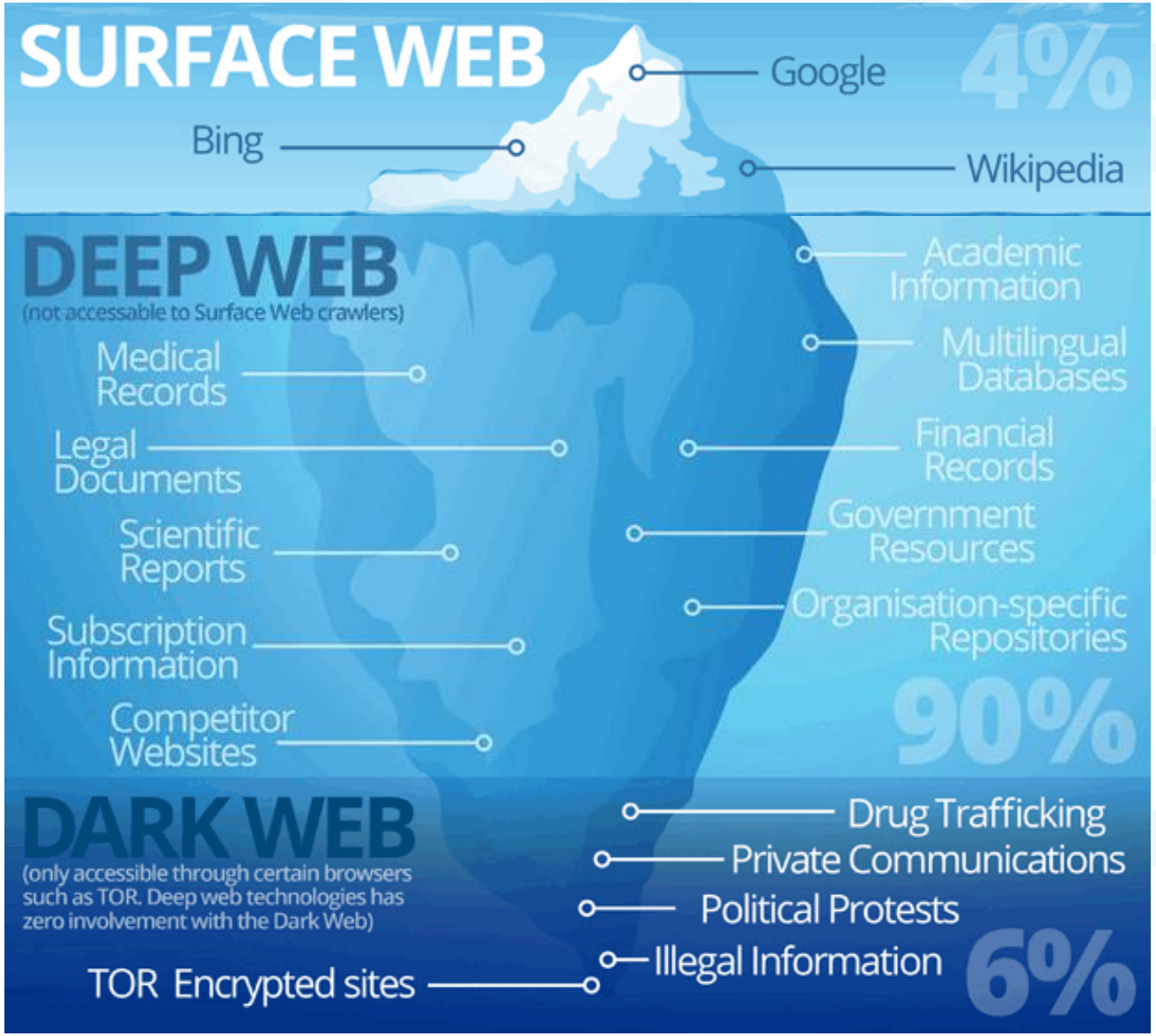
Financial Sector: Data breach cost 40% more



** Top five sectors for comparison*

Source: Ponemon Institute, Cost of Data Breach Report 2014-2018

Where does the stolen data go?



https://www.glweb.eu/blog/infografiche/item/15-difference-between-the-surface-web-the-deep-web-and-the

Credit card data

	Price in 2013	Price in 2014	Recent Prices
Visa and MasterCard (U.S.)	$4	$4	$7
Visa Classic and MasterCard (U.S.) with Track 1 and Track 2 Data	$12	$12	$15
Visa Classic and MasterCard Standard (U.K) with Track 1 and Track 2 Data	$19 – $20	$19 – $20	$40
Visa Classic and MasterCard Standard (Japan and Asia) with Track 1 and Track 2 Data	$28	$28	$50
Premium Visa and MasterCard (U.S.) with Track 1 and Track 2 Data		$23 (V); $35 (MC)	$30
Premium Visa and MasterCard (Japan and Asia) with Track 1 and Track 2 Data		$23 (V); $35 (MC)	$80 for V and MC
Premium American Express Card (U.S.) with Track 1 and Track 2 Data		$23 (V); $35 (MC)	$30
Premium Discover Card (U.S.) with Track 1 and Track 2 Data		$23 (V); $35 (MC)	$30
VBV (U.K., Australia, Canada, EU and Asia)	$17 – $25	$28	$25

https://www.secureworks.com/resources/rp-2016-underground-hacker-marketplace-report

Email and social media accounts

	Recent Prices
Popular U.S. Email Accounts (Gmail, Hotmail, Yahoo)	$129
Popular Russian Email Accounts (Mail.ru, Yandex.ru, and Rambler.ru)	$65 – $103
Popular Ukranian Email Accounts (Ukr.net)	$129
Popular U.S. Social Media Accounts	$129
Popular Russian Social Media Accounts (VK.ru and Ok.ru)	$194
Corporate Email Accounts	$500 per mailbox
IP address of Computer User	$90

https://www.secureworks.com/resources/rp-2016-underground-hacker-marketplace-report

Bank accounts and credentials

	Recent Prices
Bank Account Credentials	Price based on account balance
Bank accounts — (U.K.)	$27,003 cost $2,000
Bank account — (U.S.)	$1,000 cost $40
Bank account — (U.S.)	$2,000 cost $80
Bank account — (U.S.)	$4,000 cost $150
Bank account — (U.S.)	$7,000 cost $300
Bank account — (U.S.)	$15,000 cost $500
High Quality Bank Accounts with Verified, Large Balances of $70,000 – $150,000	6% of the balance of the account

https://www.secureworks.com/resources/rp-2016-underground-hacker-marketplace-report

Cybercrime-as-a-service

	Price in 2013	Price in 2014	Recent Prices
Hacking Tutorials	N/A	$1 each to $30 for 10 (depending on the tutorial)	$20 to $40 for multiple tutorials
Hacking Website (stealing data)	$100 – $300	$100 – $200	$350
DDoS Attacks	Per Hour: $3 – $5 Per Day: $90 – $100 Per Week: $400 – $600	Per Hour: $3 – $5 Per Day: $60 – $90 Per Week: $350 – $600	Per hour: $5 – $10 Per Day: $30-$55 Per Week: $200 – $555
Doxing	$25-$100	$25-$100	$19.99

https://www.secureworks.com/resources/rp-2016-underground-hacker-marketplace-report

Identities, passports, social security, etc.

	Price in 2013	Price in 2014	Recent Prices
US Fullz	$25	$30	$15 – $65
Fullz (Canada, U.K.)	$30 – $40	$35 – $45	$20 (Canada) $25 (U.K.)
U.K. Passport Scan			$25
Physical Counterfeit Passports (non-U.S.)	N/A	$200 – $500	$1,200 to $3,000 (European)
Physical Counterfeit Passports (U.S.)			$3,000 to $10,000
Templates for U.S. Passports			$100 – $300
New Identity Package, including scans of Social Security Card, Driver's License and, matching utility bill		$250; matching utility bill an additional $100	$90

https://www.secureworks.com/resources/rp-2016-underground-hacker-marketplace-report

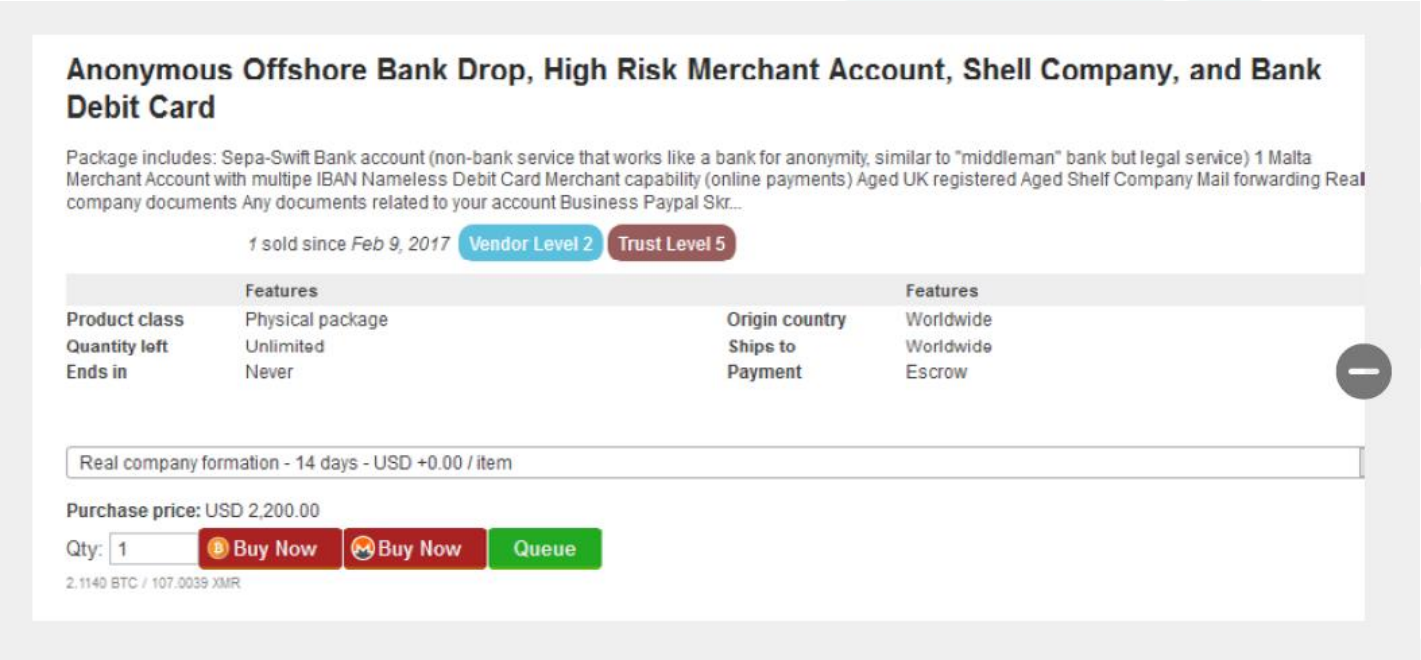
Fullz – Full set of PII

- Includes victim's financial, geographic and biographical information
- Facilitate identity theft and impersonation-based fraud
- Can include premium information e.g. passport scans, answers to "secret questions"
- Cost around US$10

https://www.secureworks.com/resources/rp-2017-state-of-cybercrime

Offshore bank drop

- Legitimate business banking accounts and documentation
- Authorized to receive and transfer more funds per transaction than personal accounts
- Easy to transfer large amounts of money in a short period of time



Anonymous Offshore Bank Drop, High Risk Merchant Account, Shell Company, and Bank Debit Card

Package includes: Sepa-Swift Bank account (non-bank service that works like a bank for anonymity, similar to "middleman" bank but legal service) 1 Malta Merchant Account with multipe IBAN Nameless Debit Card Merchant capability (online payments) Aged UK registered Aged Shelf Company Mail forwarding Real company documents Any documents related to your account Business Paypal Skr...

1 sold since Feb 9, 2017 Vendor Level 2 Trust Level 5

	Features		Features
Product class	Physical package	Origin country	Worldwide
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	Escrow

Real company formation - 14 days - USD +0.00 / item

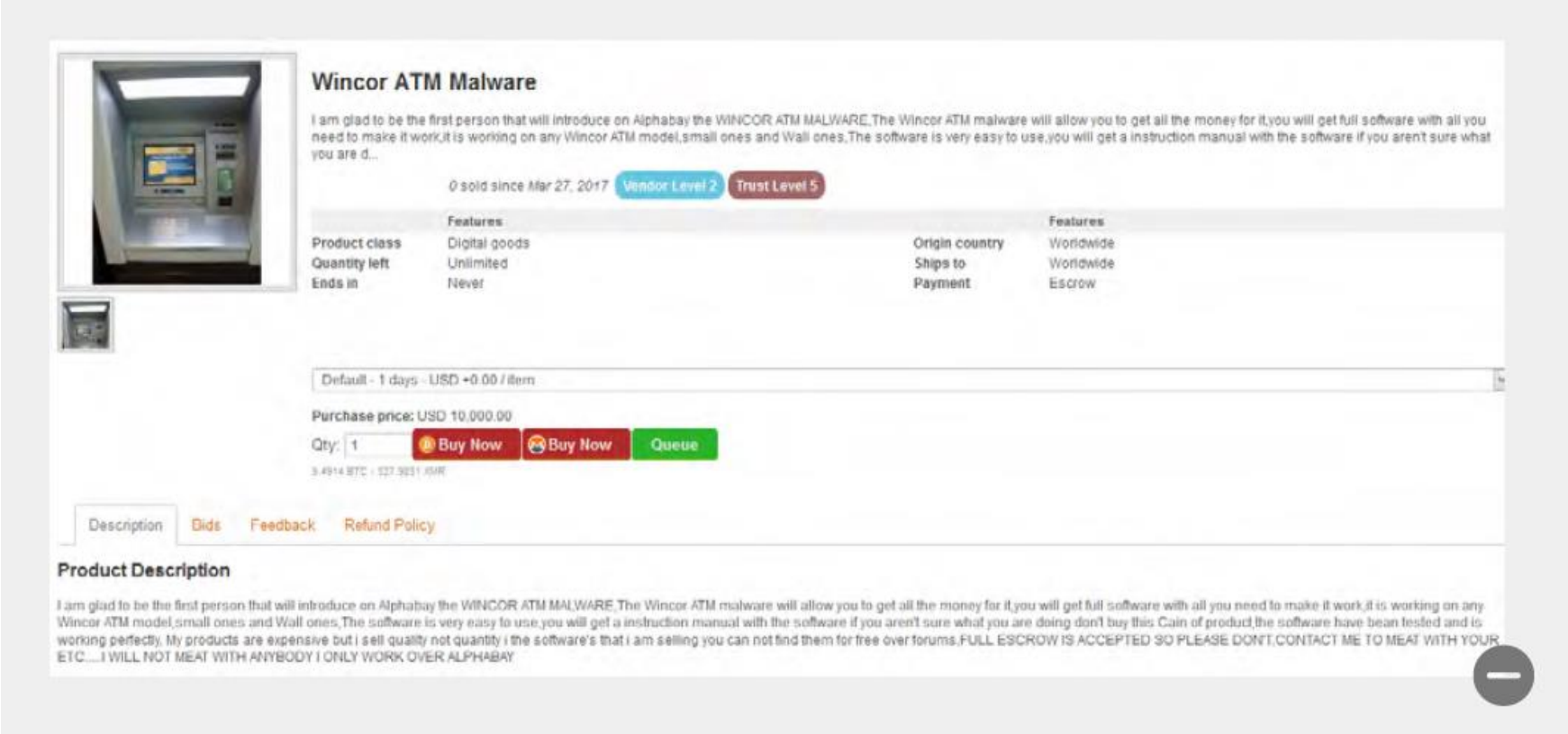
Purchase price: USD 2,200.00

Qty: 1 Buy Now Buy Now Queue

2.1140 BTC / 107.0039 XMR

https://www.secureworks.com/resources/rp-2017-state-of-cybercrime

Buy ATM “Jackpotting” Malware



Wincor ATM Malware

I am glad to be the first person that will introduce on Alphabay the WINCOR ATM MALWARE,The Wincor ATM malware will allow you to get all the money for it,you will get full software with all you need to make it work,it is working on any Wincor ATM model,small ones and Wall ones,The software is very easy to use,you will get a instruction manual with the software if you aren't sure what you are d...

0 sold since Mar 27, 2017 | Vendor Level 2 | Trust Level 5

	Features		Features
Product class	Digital goods	Origin country	Worldwide
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	Escrow

Default - 1 days - USD +0.00 / item

Purchase price: USD 10,000.00

Qty: 1 | Buy Now | Buy Now | Queue

Description | Bids | Feedback | Refund Policy

Product Description

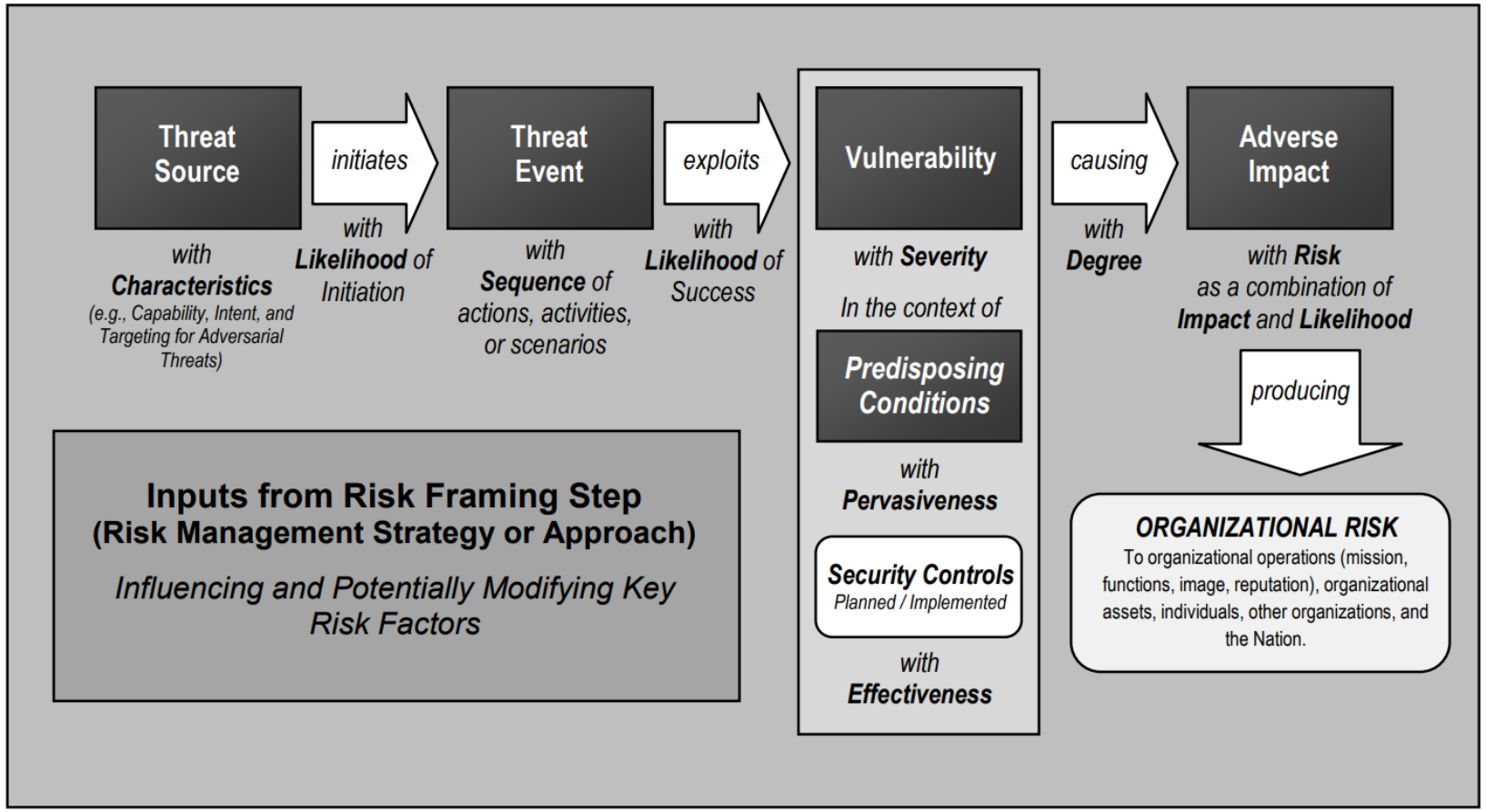
I am glad to be the first person that will introduce on Alphabay the WINCOR ATM MALWARE,The Wincor ATM malware will allow you to get all the money for it,you will get full software with all you need to make it work,it is working on any Wincor ATM model,small ones and Wall ones,The software is very easy to use,you will get a instruction manual with the software if you aren't sure what you are doing don't buy this Cain of product,the software have bean tested and is working perfectly, My products are expensive but i sell quality not quantity i the software's that i am selling you can not find them for free over forums,FULL ESCROW IS ACCEPTED SO PLEASE DON'T,CONTACT ME TO MEAT WITH YOUR ETC.....I WILL NOT MEAT WITH ANYBODY I ONLY WORK OVER ALPHABAY

https://www.secureworks.com/resources/rp-2017-state-of-cybercrime

You Have Either Been Hacked or Will Be

SWARMNETICS

Threats exploits vulnerabilities to cause harm



https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Know Your Enemy

How powerful are they? (capability)

Who are these barbarians? (source)

What do they want? (intent)

How badly do they want it? (motivation)

- Make a name in the hacker scene
- Happy with the acquired knowledge
- No real target, anything will do, preferably well-known (e.g. Facebook, Google, …)

Just for Fun!

Hacktivism

- Social or political motive
- Targets at governments or large companies
- Attacker wants high visibility (e.g. defacing, DoS, …)

Cybercrime

- Driven by profits, make as much as possible in the shortest time
- Target personally identifiable information (PII) and critical resources
- Use direct attacks at system (e.g. application, payment, ATM, …)

CYBERCRIME DEPENDENCIES MAP

Crypting
Encrypting and/or packing files to obfuscate them from security software

Automatic Vending Cart (AVC)
Automated 'click-and-buy' websites selling compromised data (typically credit card data)

Reselling (Data)
A data vendor who buys bulk (compromised) data and re-sells it in smaller volumes

Counter Anti-Virus
Testing of malware samples to determine if they are detected by commercial anti-virus products

Exploits
Research or design of exploits to abuse vulnerabilities in browsers and other software in order to install malware

Carding
Using compromised credit cards to fraudulently purchase goods and services

Translation
Translation into a target/victims native tongue to increase authenticity and attack success

Coding
Authoring/creating malware for use by others such as Trojans, RATs, etc

Pay-Per-Install
Paid for each download and launch of a clients software/malware

Mules/Drops
Provide accounts or addresses for the receipt of stolen or fraudulently obtained goods or funds

Mule Herding
Recruits and runs teams of mules

Malware Deployment
Deploying/running malware to create botnets, harvest data, gain unauthorised access, etc

Traffic
A service directing visitors to a specific (typically compromised/ infected) website

Fake Documents / IDs
Fake or fraudulently obtained genuine documents for use in fraud

Spam
Mass distribution of unsolicited communications (email, SMS, etc) which often contain malicious payloads or links

Inject Writing
Custom injects which allow malware users to modify specific webpages to extract or add additional data

Denial of Service (DoS) Attacks
Blocking legitimate access to a victim website/server by flooding it with traffic

Web Design
Production of web content by a suitably skilled designer

Cross-Crime Factors

Hosting (Bulletproof)
Dedicated/shared/virtual hosting which may be non-compliant to law enforcement requests

Forums
Online bulletin boards used as meeting places and markets by cybercriminals to sell products/ services

Domain Services
Provision of generic and countrycode Top Level Domains (gTLDs and ccTLDs)

VPN / Proxy Services
Anonymising services which masks a user's original IP address and can encrypt their internet traffic

Currency Exchange
Exchange between virtual and other (virtual or fiat) currencies

Mixer / Tumbler
A money-laundering service which hides a virtual currency financial trail by pooling and redistributing clients funds

Secure Communications
Secure (e.g. encrypted, un-logged) email and/or instant messaging

The **Cybercrime Dependencies Map** is designed to outline the key products and services within the digital underground and to highlight how and to what degree these products and services are *DEPENDENT* on each other to operate. For example, **Mule Herding** has a *HIGH DEPENDENCY* on the availability of **Mules**.

Several products or services are commonly required by many other services in order for them to operate. These have been collected under **Cross-Crime Factors**. Where one of these **Cross-Crime Factors** has been assessed as being of *HIGH* or *MEDIUM* importance to some of the key products/services it has been allocated an icon in order to annotate the appropriate product/ service.

Mouse over the arrows to see the level of dependency between products and/or services.

LEGEND

Highly dependent on - Cannot do without

Key product/service but not essential

'Optional' service

Product/Service
Product/Service Description
Cross-Crime Factors upon which this service has a High/Medium dependence

Product
Where the customer is required to do everything themselves after purchase

Service
Where a product involves on-going interaction or is run and maintained by someone else

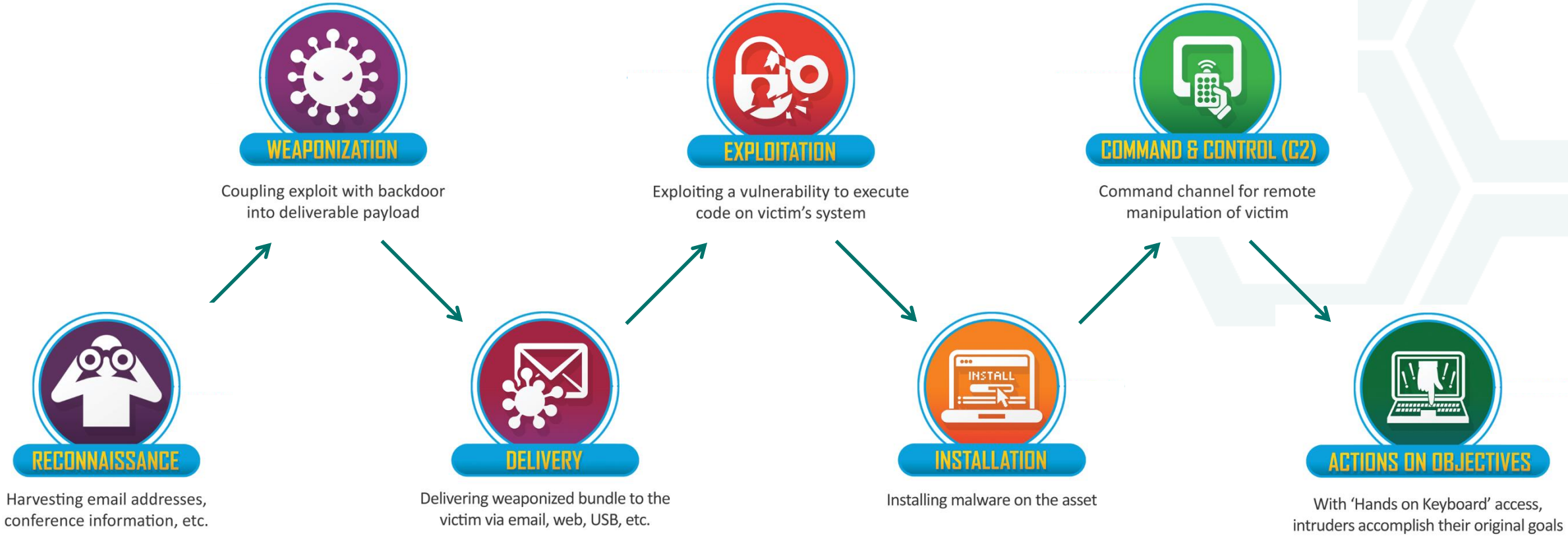
EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

- Motivated by political, economic, or military agendas
- Well-funded and use sophisticated, targeted attacks
- Not interested in short-term gains, but wants long-term foothold
- Target large organizations or critical infrastructure

State Sponsored

Know Your Enemy

Cyber Kill Chain – Sophisticated, Persistent



https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

Reconnaissance – Identify the Targets

Harvesting email addresses, conference information, etc.

- Harvest email addresses
- Identify employees on social media networks
- Collect press releases, conference attendee lists, etc
- Discover internet-facing systems

Weaponization – Prepare the Operation

Coupling exploit with backdoor into deliverable payload

- Identify vulnerability to exploit
- Package malware – exploit and backdoor (“payload”)
  - Exploit: Means to obtain control by attacking the vulnerability
  - Backdoor: Provides attacker with access to the system
- Setup command and control (C2) infrastructure

Delivery – Launch the Operation

Delivering weaponized bundle to the victim via email, web, USB, etc.

- Deliver the malware to the target
  - Attack the web servers
  - Send malicious email
  - Drop USB stick (with malware)
  - Interact through social media (e.g. malicious link)
  - “Watering hole” websites (i.e. infect sites where victims gather)
  - …

Exploitation – Gain Access to Victim

Exploiting a vulnerability to execute code on victim's system

- Exploit software, hardware, or human vulnerability
- Attacker triggered
  - Exploit vulnerability on system (e.g. website)
- Victim triggered
  - Open email with malicious attachment
  - Click malicious link
  - Insert malicious USB stick

Installation – Establish Beachhead

Installing malware on the asset

- Install backdoor on the victim
- Create point of persistence (e.g. autorun a service)
- Make malware appear as part of system

Command & Control (C2) – Remote Control

Command channel for remote manipulation of victim

- Open communications channel to C2 infrastructure
- Usually over web, DNS and email protocols
- C2 infrastructure may be owned by the attacker or sitting on another victim network

Action on Objectives – Achieve the Goal

With 'Hands on Keyboard' access, intruders accomplish their original goals

- Collect user credentials
- Privilege escalation (i.e. gain higher access rights)
- Internal reconnaissance (i.e. gather more information)
- Lateral movement through environment (i.e. exploit more victims to move towards "bigger" target)
- Collect and exfiltrate data
- Destroy systems or delete data
- Overwrite, corrupt or modify data or transactions

In reality based on actual breaches …

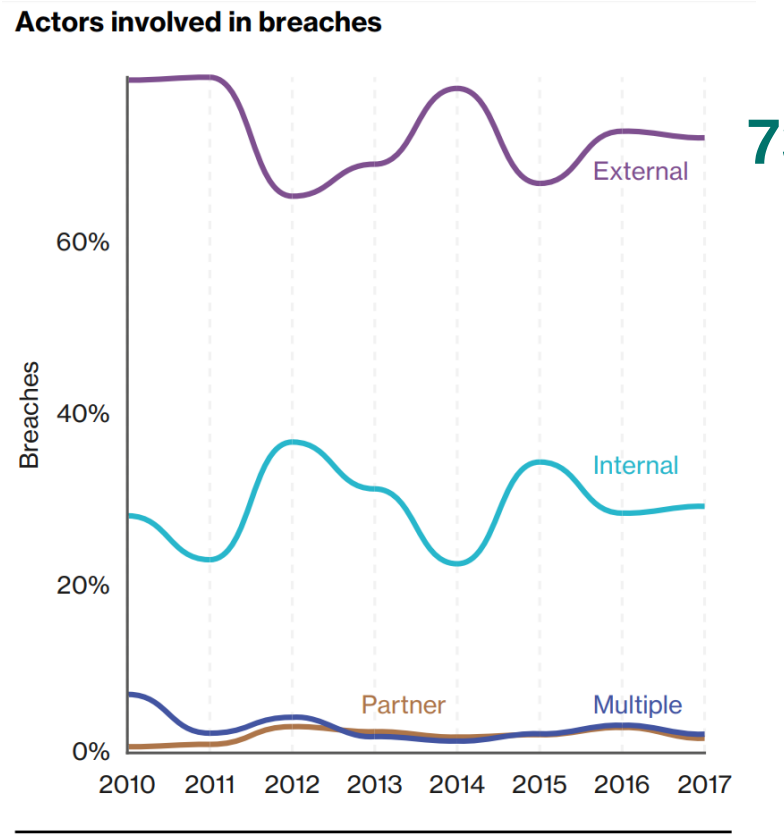


Figure 1. Threat actors within breaches over time

73%

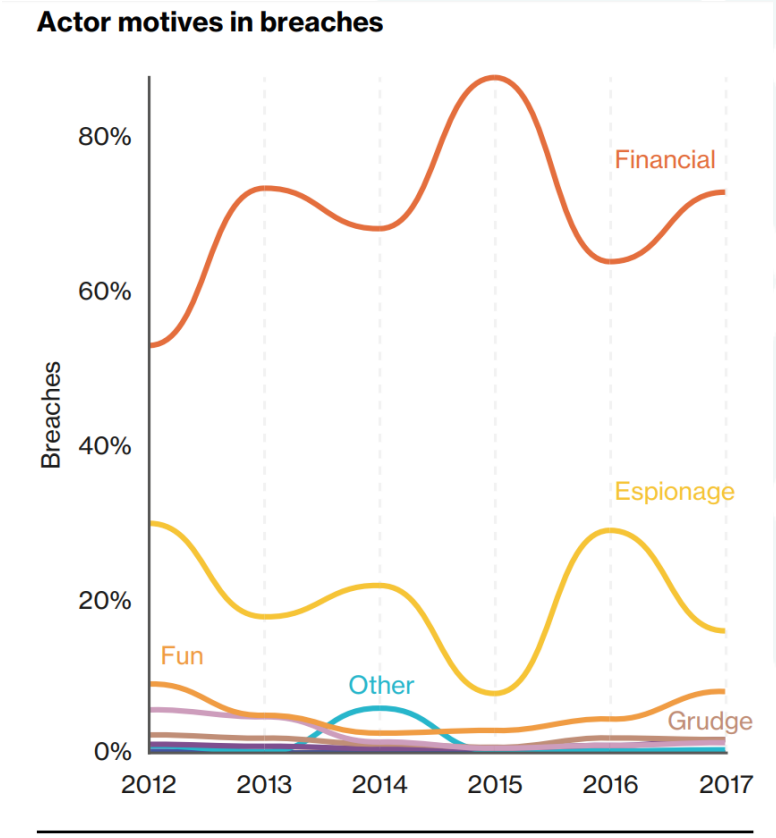


Figure 2. Threat actor motives within breaches over time

76%

https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf

How the bad guys get in …

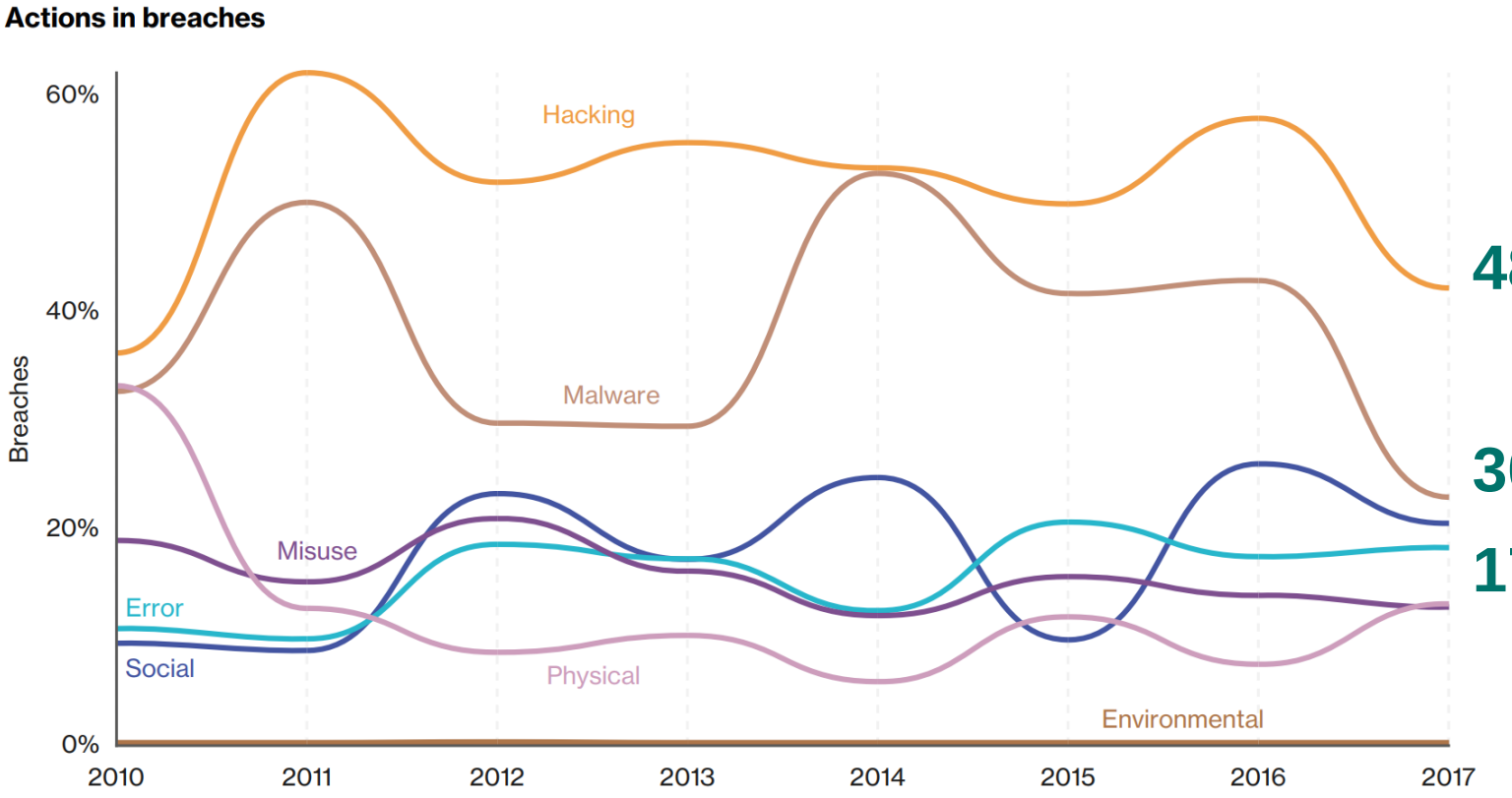


Figure 3. Percentage of breaches per threat action category over time

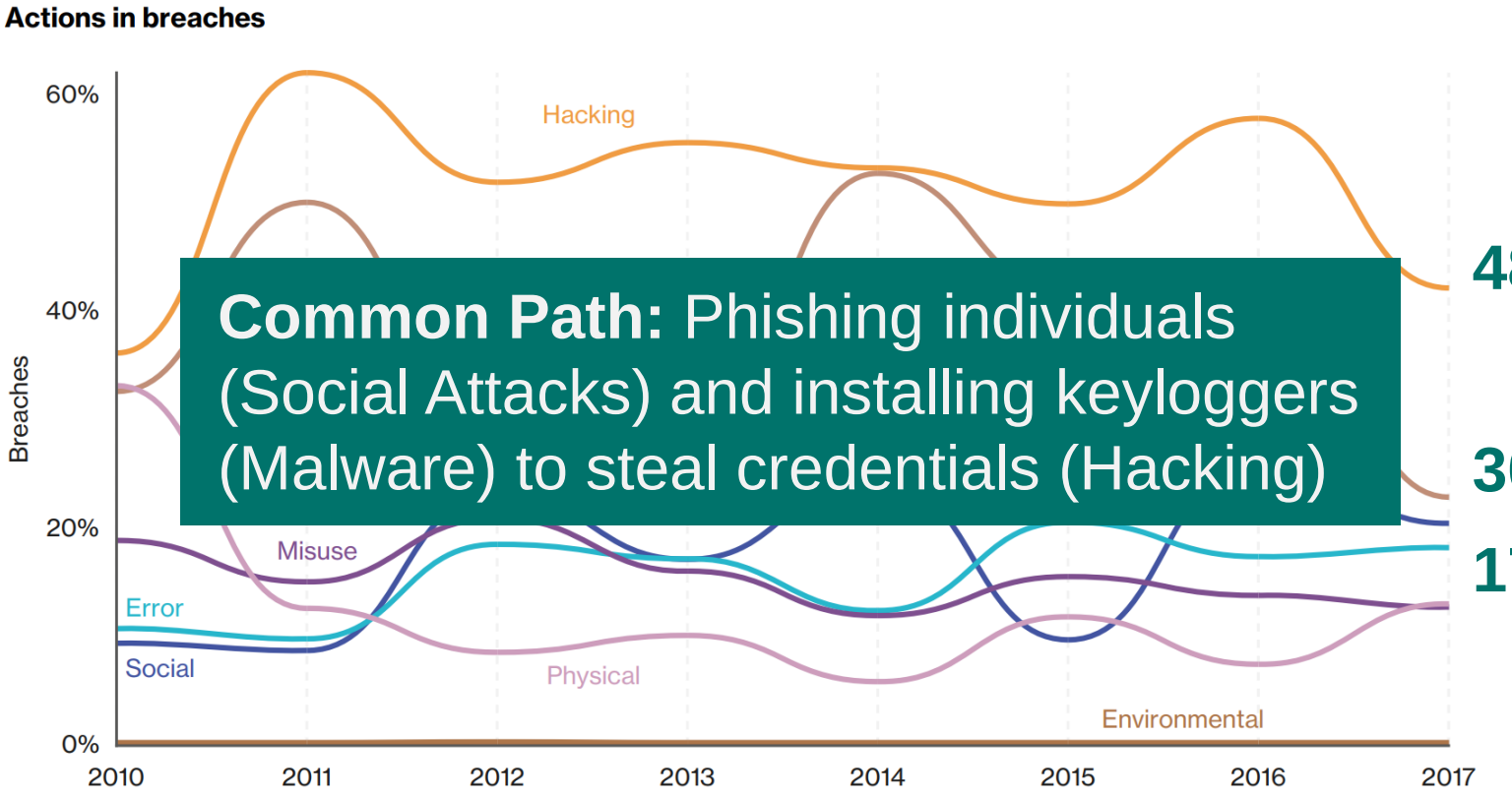
48% Hacking

30% Malware

17% Social Attacks

https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf

How the bad guys get in …



Common Path: Phishing individuals (Social Attacks) and installing keyloggers (Malware) to steal credentials (Hacking)

48% Hacking

30% Malware

17% Social Attacks

Figure 3. Percentage of breaches per threat action category over time

https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf

Phishing & pretexting – 90% of social attacks

Pretexting attacks targeting employees in finance or HR:

> Impersonates C-level executive and influence Finance staff to transfer money (typically 6-figures)

> Targets HR information (e.g. salary, etc.) to file fraudulent tax returns on behalf of employees and deposit refunds to attackers' account

```
Received: from vps-1108036-11644.manage.myhosting.com
(vps-1108036-11644.manage.myhosting.com [216.224.172.98])
        [redacted]
        [redacted]>; Mon, 4 Jan 2016 22:18:08 GMT
Received: from isdcac by vps-1108036-11644.manage.myhosting.com with local (Exim 4.86)
        (envelope-from <[redacted]@[redacted].com>)
        id 1aGDS2-0005oU-GL
        for [redacted]; Tue, 05 Jan 2016 03:48:06 +0530
To: [redacted]
Subject: Please get back to me on this
X-PHP-Script: dear.isdc.ac.in/lsysxx.php for 69.129.222.142
From: "[redacted]" <[redacted]@[redacted].com>
Reply-To: [redacted]@[redacted].com
MIME-Version: 1.0
X-Mailer: PHPMailer [version 1.72]
X-Priority: 1
Content-Type: text/plain
Content-Transfer-Encoding: 8bit
Message-Id: <E1aGDS2-0005oU-GL@vps-1108036-11644.manage.myhosting.com>
Date: Tue, 05 Jan 2016 03:48:06 +0530

Do you have a moment?  I am tied up in a meeting and there is something i need you to
take care of.

We have a pending invoice from our Vendor. I have asked them to email me a copy of the
invoice and i will appreciate it if you can handle it before the close of banking
transactions for today.

I cant take calls now so an email will be fine.

Sent from my iPhone
```

Spoofed email address

Phishing & pretexting – 90% of social attacks

Phishing baits victims to

> Open malicious attachment

> Click on link to a page that request credentials or drop malware

4%	of recipients will click/open (attacker just needs one)
16m	to first click in most campaigns
59%	financially motivated
41%	motivated by espionage
70%	of state-sponsored breaches

From: AppIe ID <id.apple.2966@secureforclick.com>
Date: May 13, 2017 at 4:16:57 PM EDT
To: undisclosed-recipients:;
Subject: Order #HD923480 Confirmed

Invoice

Thank you for buying			
INVOICE DATE 13 Mei 2017		BILLED TO Apple Store	TOTAL $109,99
ORDER ID M2MNSYJ0102	DOCUMENT NO. 175116838085		

App Store	TYPE	PURCHASED FROM	PRICE
 **iTunes Gift Card** Cancel Order	Purchase In-App	iPhone	**$109,99**

TOTAL **$109,99**

If you did not authorize this purchase, please visit iTunes Payment Cancellation

Click here to Cancellation Payment

Apple ID Summary â€¢ Purchase History â€¢ Terms of Sale â€¢ Privacy Policy

Copyright Â© 2017 Apple Inc.
All rights reserved

From: Apple <hellowmesian@oscaer.com>
Date: May 17, 2017 at 9:29:21 AM EDT
To: [redacted]
Subject: Alert: You've made changes from an unauthorised devices.

Dear Client,

Your Apple ID has been locked for security reasons.
Someone logged into your Apple ID from a different IP address.

Date and Time: 16 May 2017, 10:27 AM BST
Browser: Firefox
IP: 90.148.227.40 (Dhaka, Bangladesh)
Operating System: Windows

We need to verify your account in order to continue using your Apple ID.

Click here to Confirm
Please do not reply to this email. If you need any additional help, visit Apple Support.

Sincerely,

Apple Support

Apple ID | Support | Privacy Policy
Copyright ◆ 2017 Apple Distributions International Ltd. All rights reserved.

Hope you have not seen this screen

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:

   74fZ96-2Nx1Gm-yHQRWr-S8gaN6-8Bs1td-U2DKui-ZZpKJE-kE6sSN-o8tizV-gUeUMa

If you already purchased your key, please enter it below.
Key: _

Ransomware – 56% of malware attacks

US$41.5M sales (excl. held inventory and halted production)

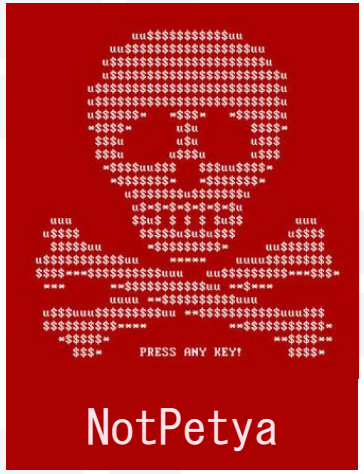
US$117M sales (Reckitt Benckiser owns Dettol, Durex)

US$290M sales (French building manufacturer)

US$300M business cost (incl. reinstall 4K servers, 45K PCs)

US$300M operating cost

US$310M sales and operating costs (expect to double)



Financial and insurance sector

- Most common – Banking Trojan botnets and Denial of Service
- “Everything else” – Phishing accounts for more than half of incidents
- “Crimeware” – Ransomware is top
- “Web applications” – Hacking

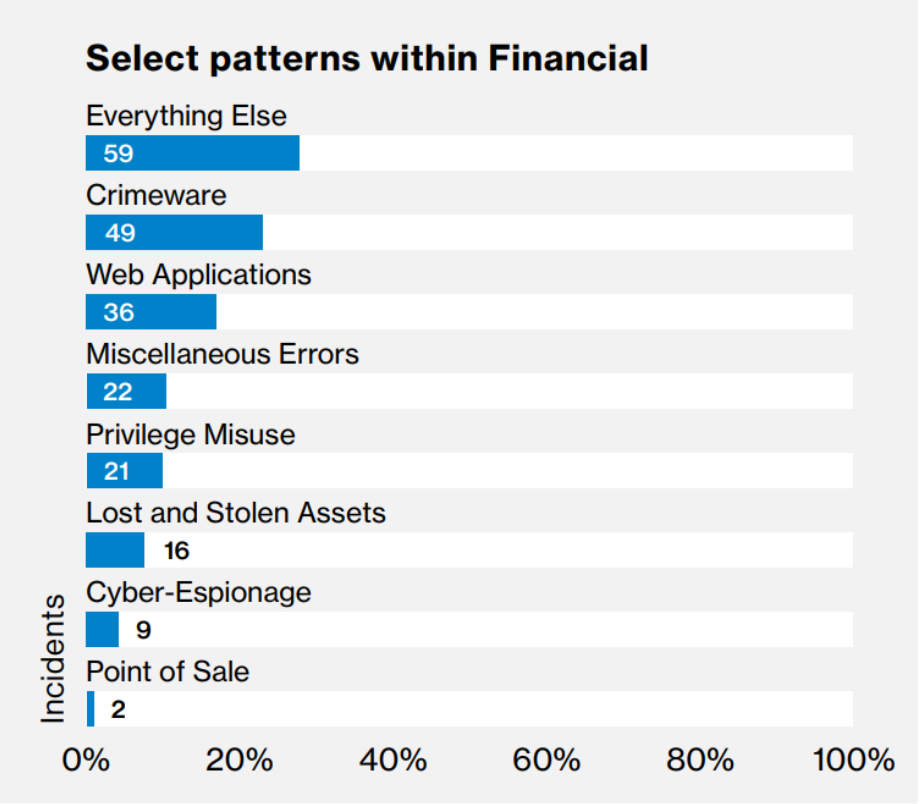


Figure 31. Incident classification patterns within select Financial and Insurance industry incidents (n=213)

How bank trojans typically works

1. Victim infected by malicious email attachment (“phishing”) or by visiting a compromised/infected website (“drive-by downloads”)
2. Trojan identifies when victim is visiting a banking website.
3. Trojan captures victim’s credentials
   - Use keylogging to record data
   - Add extra fields to web forms (e.g. capture victim’s PIN)
   - Change website wording or trigger popup forms

OR

3. Trojan authenticates session, and criminals perform transactions
   - Redirect victim to fake website that resembles legitimate site
   - Victim enters credentials (incl. SMS or other 2FA code) in fake website, and trojan enters them into the legitimate site.

https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=77014377USEN

Case Study: Equifax Breach 2017

Equifax

Credit bureau providing credit monitoring and fraud-prevention services. Aggregates data of 800M consumers and 88M businesses.

CIO & CISO resigns **Sep 16**

CEO resigns **Sep 26**

Mid-May

Hackers download data

Jul 29

Discovered data breach

Sep 7

Equifax disclose data breach

Slow detection and long notification period

Impact

Compromised data out in the market for 17 weeks and identity fraud, etc. may have already occurred.

Mid-May

Hackers download data

Jul 29

Discovered data breach

Sep 7

Equifax disclose data breach

Ineffective security patch management

Critical Apache Struts vulnerability found and patch released next day

Mar 7

Admitted they knew about the patch and had attempted to apply it to all their systems.

Patch applied on system

Jul 30

21 weeks

Mid-May

Hackers download data

Jul 29

Discovered data breach

Sep 7

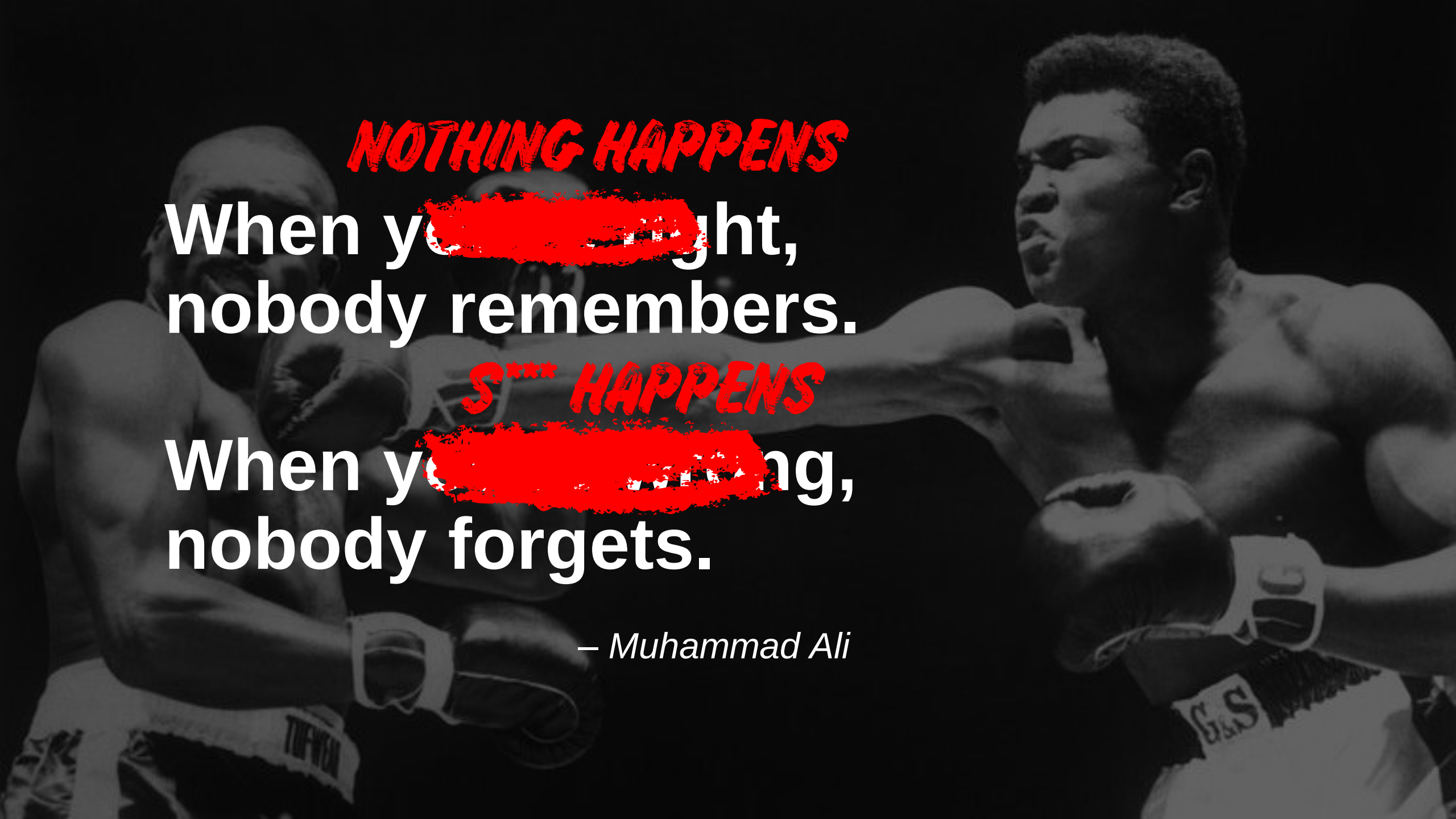
Equifax disclose data breach

Poorly orchestrated breach response

1. Directed potential victims to a separate domain (equifaxsecurity2017.com) instead of main, trusted website (equifax.com)
   - Bugs were found on the site
   - Developer Nick Sweeting set up securityequifax2017.com to show how site can be spoofed
   - Tweeted the fake link 4 times by mistake
2. Calls to dedicated hotline unanswered
3. Customers offered free credit monitoring services but by doing so, waive their rights to sue

Keeping the Barbarians Outside the Gate

SWARMNETICS


NOTHING HAPPENS
When y[redacted]ght,
nobody remembers.
S*** HAPPENS
When y[redacted]ng,
nobody forgets.
– Muhammad Ali

1 Attacker’s Advantage

– Bad Guys need one hole, Good Guys need to cover all holes

Exponential rise in software vulnerabilities

31% increase in vulnerabilities in 2017

17% of more than 20K vulnerabilities in 2017 rated as critical

38% of reported vulnerabilities in 2017 did not received a CVE ID → excluded from most vulnerability scanners

https://www.riskbasedsecurity.com/2018/02/7900-vulnerabilities-in-2017-you-arent-aware-of-may-put-your-organization-at-risk/
https://puppet.com/resources/whitepaper/state-of-devops-report

2 Resource constraints

– Budget and workforce shortage

Cybersecurity Workforce Gap – 1.8M by 2022

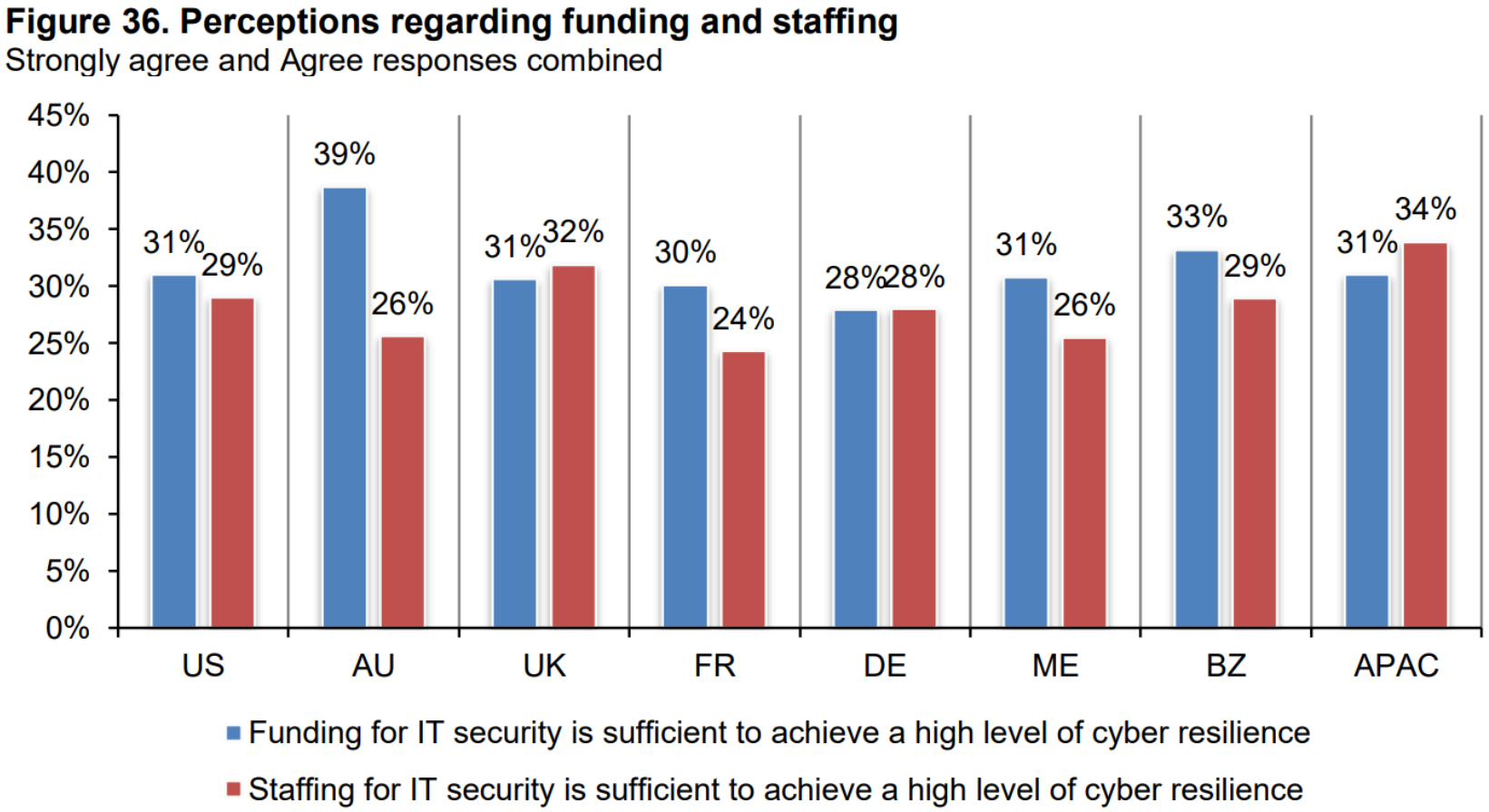
66% recognize they **do not have enough** staff to address current threats

68% believe there is a **lack of qualified** personnel

70% want to **increase size** of cybersecurity staff

https://www.isc2.org/News-and-Events/Press-Room/Posts/2017/06/07/2017-06-07-Workforce-Shortage

Only 31% say cybersecurity budget sufficient



https://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2018_Cyber_Resilient_Organization_Study.pdf

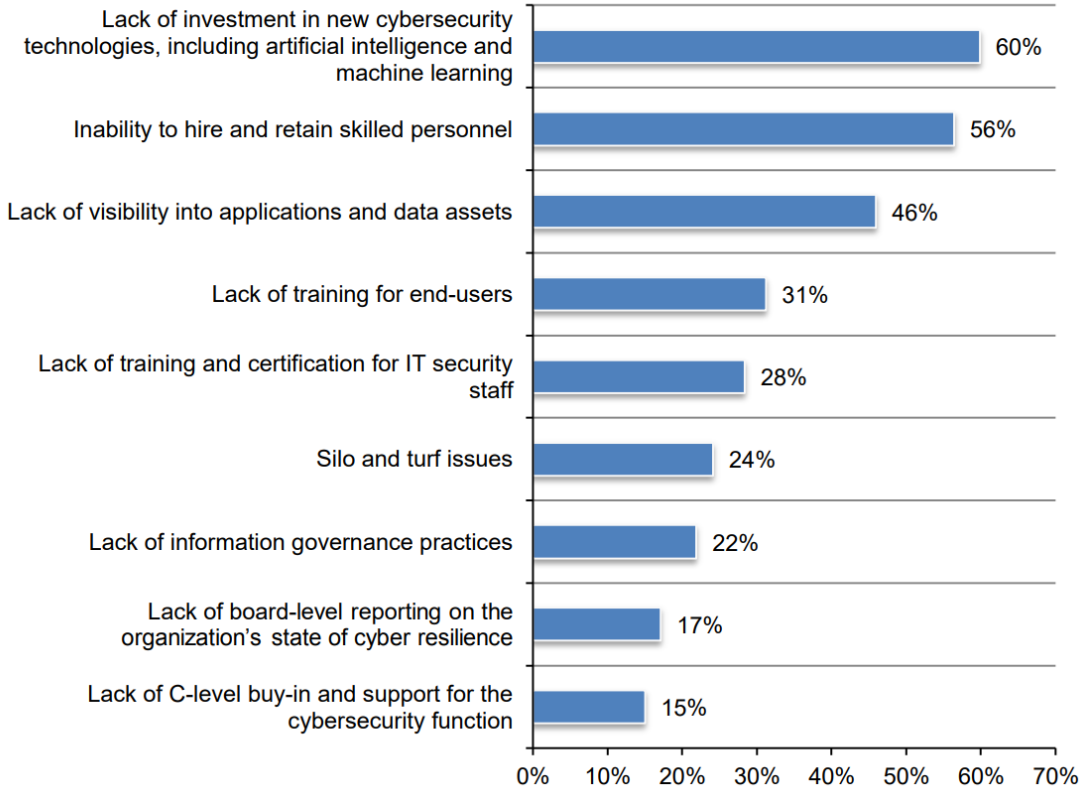
3

Limited Visibility

– Not knowing your weaknesses and how well you are doing

46% lack visibility

Figure 8. What are the biggest barriers to cyber resilience?
Three choices allowed



https://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2018_Cyber_Resilient_Organization_Study.pdf

Useful guiding principles for cyber defense

1. **Offense informs defense**
   - > Use actual attacks for continual learning
   - > Build effective and practical defense
   - > Focus only on controls proven to stop known real-world attacks

Useful guiding principles for cyber defense

1. **Offense informs defense**
2. **Active prioritization**

> Invest first in controls that provides greatest risk reduction and protection

> Focus on controls that can be feasibly implemented in your environment

> Establish common metrics to provide a shared language across organization

Useful guiding principles for cyber defense

1. **Offense informs defense**
2. **Active prioritization**
3. **Continuous diagnostics**

> Measure the effectiveness of cyber defense for rapid iteration

> Continuously test and validate effectiveness of current security defense

> Continuously identify vulnerabilities and weaknesses

What to do?

1. Use a recognized framework for guidance
2. Understand your organization's cyber maturity and what is needed
3. Know your vulnerabilities – people, process, technology
4. Prioritize ("must do" over "good to do") controls based on real-world effectiveness against real-world attacks
5. Automate and orchestrate as far as possible

Assess and measure continuously to increase effectiveness

① Use a recognized framework for guidance

a. ISO/IEC 27001 and 27002 Information security management systems
b. ISF Standard of Good Practice for Information Security
c. NIST Cybersecurity Framework
d. CIS Controls
e. New York Department of Financial Services Cybersecurity Regulations
f. COBIT 5
g. NAIC Insurance Data Security Model Law

NIST Cybersecurity Framework (CSF)

- First released in Feb 2014, directed by Obama's Executive Order (EO) 13636
- Created through industry and government collaboration
- Prioritized, flexible, repeatable and cost-effective approach
- Gartner forecasts 50% adoption (U.S.) by 2020
- Latest version 1.1 released April 2018

Consists of 5 functions

Functions				
IDENTIFY	**PROTECT**	**DETECT**	**RESPOND**	**RECOVER**
Develop an organizational understanding to **manage cybersecurity risk** to systems, people, assets, data, and capabilities.	Develop and **implement appropriate safeguards** to ensure delivery of critical services.	Develop and implement appropriate activities to **identify the occurrence** of a cybersecurity event.	Develop and implement appropriate activities to **take action regarding a detected cybersecurity incident**.	Develop and implement appropriate activities to maintain plans for resilience and to **restore any capabilities or services** that were impaired due to a cybersecurity incident.

Provides a set of activities to achieve specific cybersecurity outcomes

23 categories and 108 subcategories

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Categories (Groups of Outcomes)				
> Asset Management > Business Environment > Governance > Risk Assessment > Risk Management > Strategy Supply Chain Risk Management	> Identity Management, Authentication and Access Control > Awareness and Training > Data Security > Information Protection Processes and Procedures > Maintenance > Protective Technology	> Anomalies and Events > Security Continuous Monitoring > Detection Processes	> Response Planning > Communications > Analysis Mitigation Improvements	> Recovery Planning > Improvements > Communications
Subcategories (Specific Activity Outcomes)				

CIS Controls™ – Top 20

- Prioritized set of actions
- Mitigate the most common attacks
- Developed by a community from wide range of sectors
- Based on first-hand experience
- Started as grassroots effort to cut through “more is better” thinking

Basic CIS Controls

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational CIS Controls

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational CIS Controls

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

Basic Controls (47 sub-controls)

Basic CIS Controls

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

- Should be among the very first things to be done
- Create a strong foundation for your defense
- Referred to as “Cyber Hygiene”

Foundational Controls (88 sub-controls)

Foundational CIS Controls

7	Email and Web Browser Protections	8	Malware Defenses
9	Limitation and Control of Network Ports, Protocols and Services	10	Data Recovery Capabilities
11	Secure Configuration for Network Devices, such as Firewalls, Routers and Switches	12	Boundary Defense
13	Data Protection	14	Controlled Access Based on the Need to Know
15	Wireless Access Control	16	Account Monitoring and Control

Organizational Controls (36 sub-controls)

Organizational CIS Controls

17 Implement a Security Awareness and Training Program

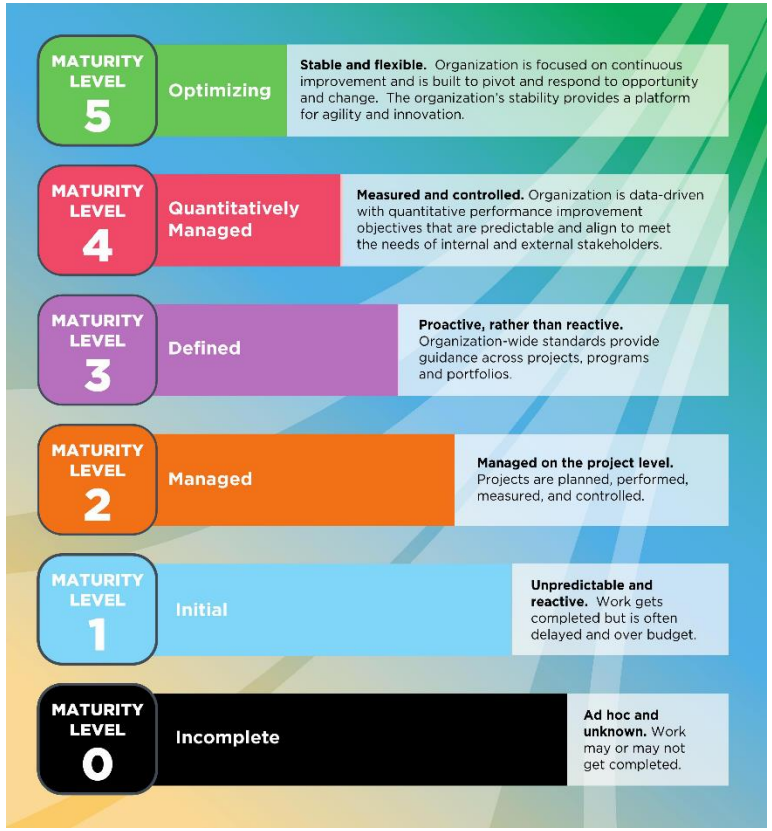
18 Application Software Security

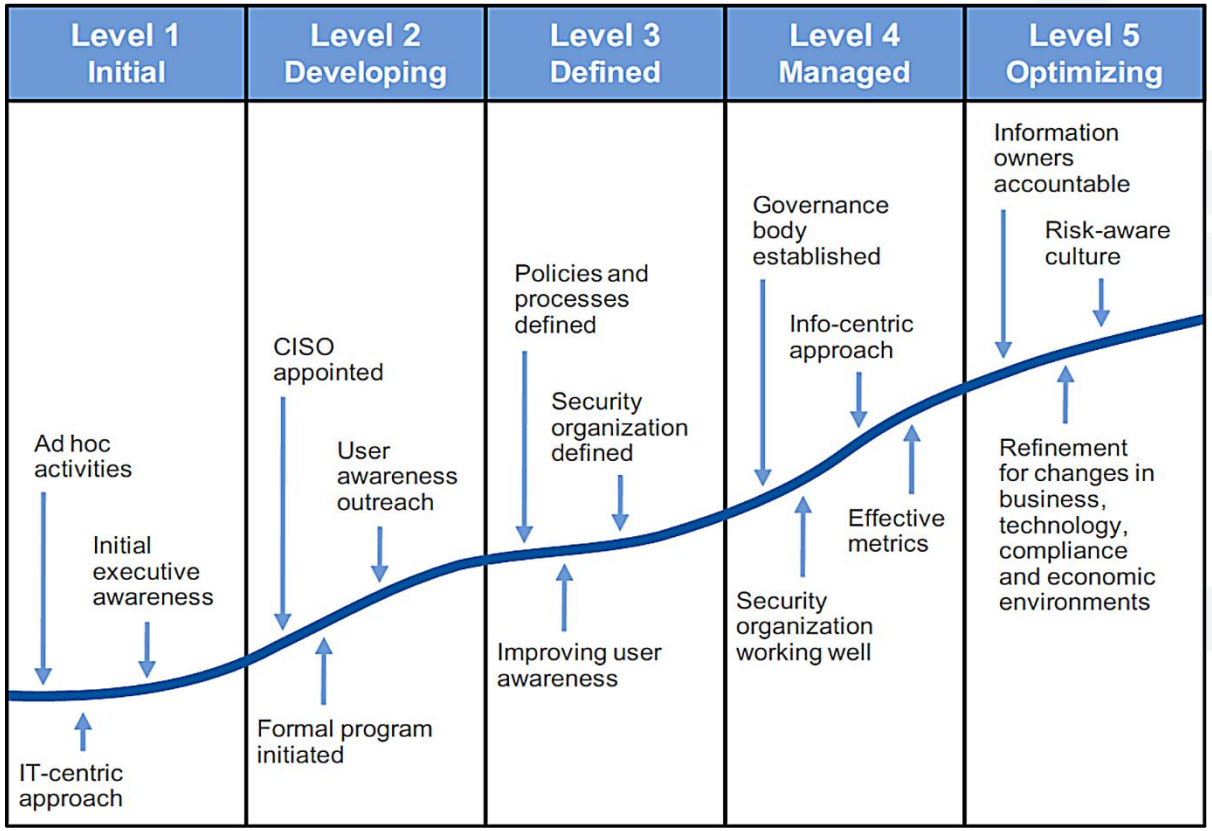
19 Incident Response and Management

20 Penetration Tests and Red Team Exercises

- Foundational part of cyber defense program
- More focused on people and processes
- Pervasive across the entire enterprise

② Understand your organization's cyber maturity and what is needed





https://www.sans.org/reading-room/whitepapers/analyst/curve-maturity-model-endpoint-security-36342
https://cmmiinstitute.zendesk.com/hc/en-us/articles/360000175667-How-is-CMMI-V2-0-different-from-V1-3-

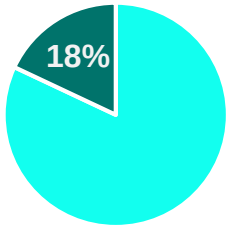
3 Know your vulnerabilities – people, process, technology

Train, test and repeat

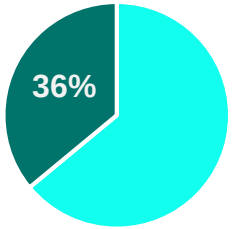
- Focus on areas of weaknesses
- Customized based on user groups – developers, HR, finance, etc.
- Bite-sized information through variety of channels – mobile, video, images, etc.
- Increase engagement – gamification, social, challenges, incentives, etc.
- Continuous delivery and update
- Measure effectiveness and retention

Phishing simulations

Users who click

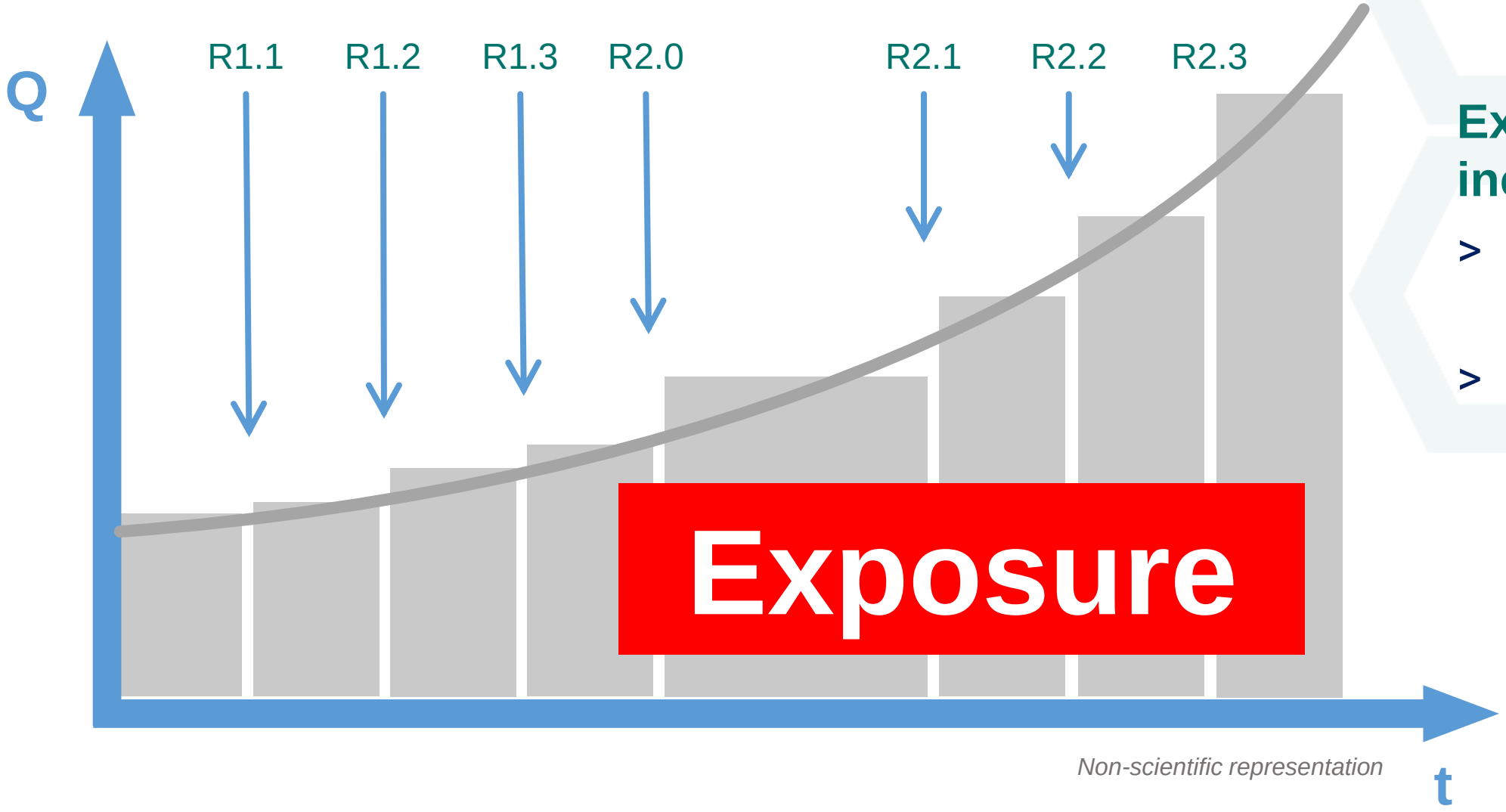


Users who submit credentials



Failure Rate	General Recommendations
0 – 10%	Targeted reminders to offenders
11 – 25%	Phishing awareness email reminder across entire organization
26 – 50%	Phishing awareness email reminder across entire organization and training for high-risk job functions
51 – 75%	Phishing awareness email reminder and training across entire organization
76 – 100%	Phishing awareness program across entire organization

Software vulnerabilities unavoidable

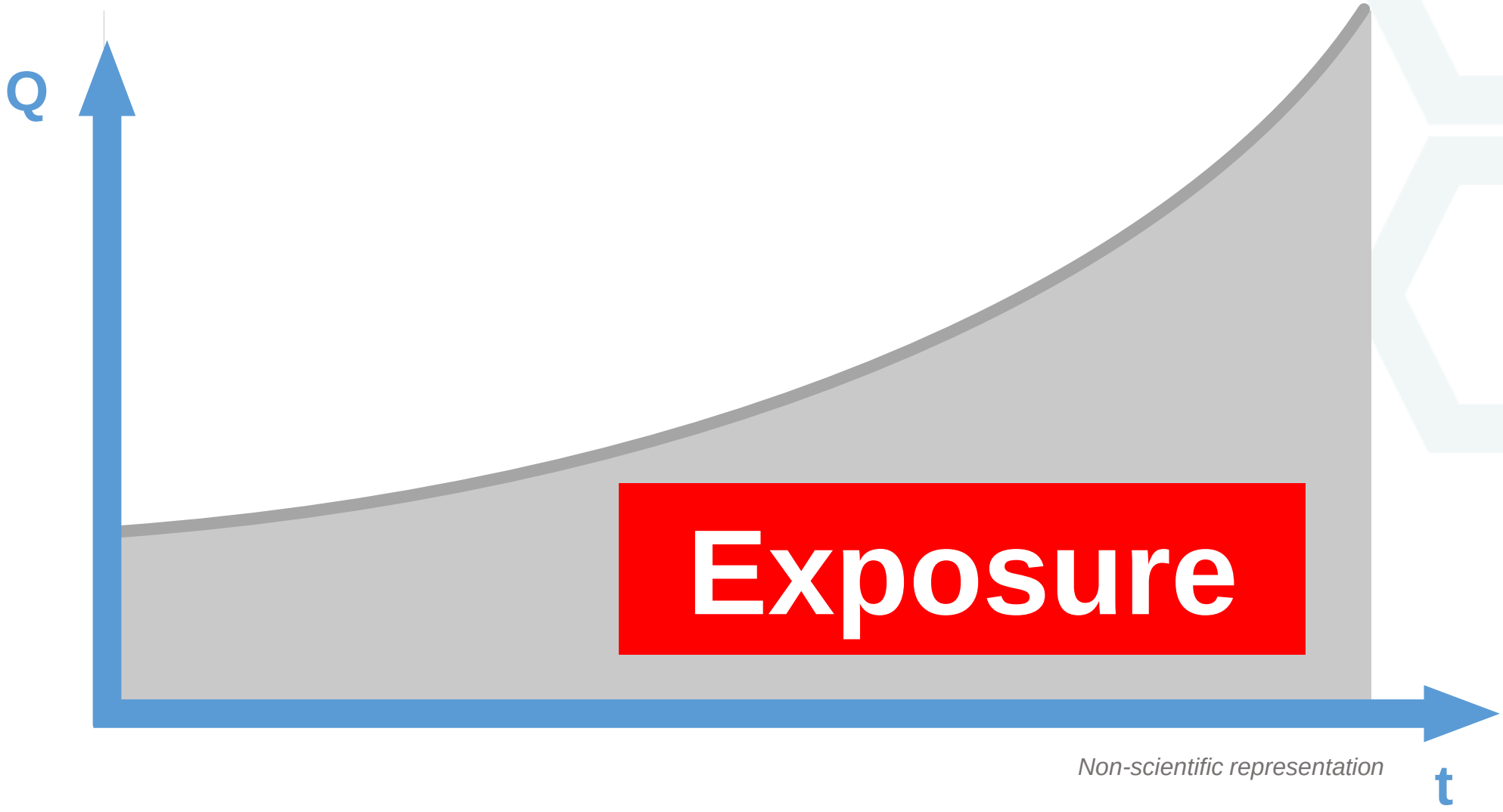


Non-scientific representation

Exponential increase

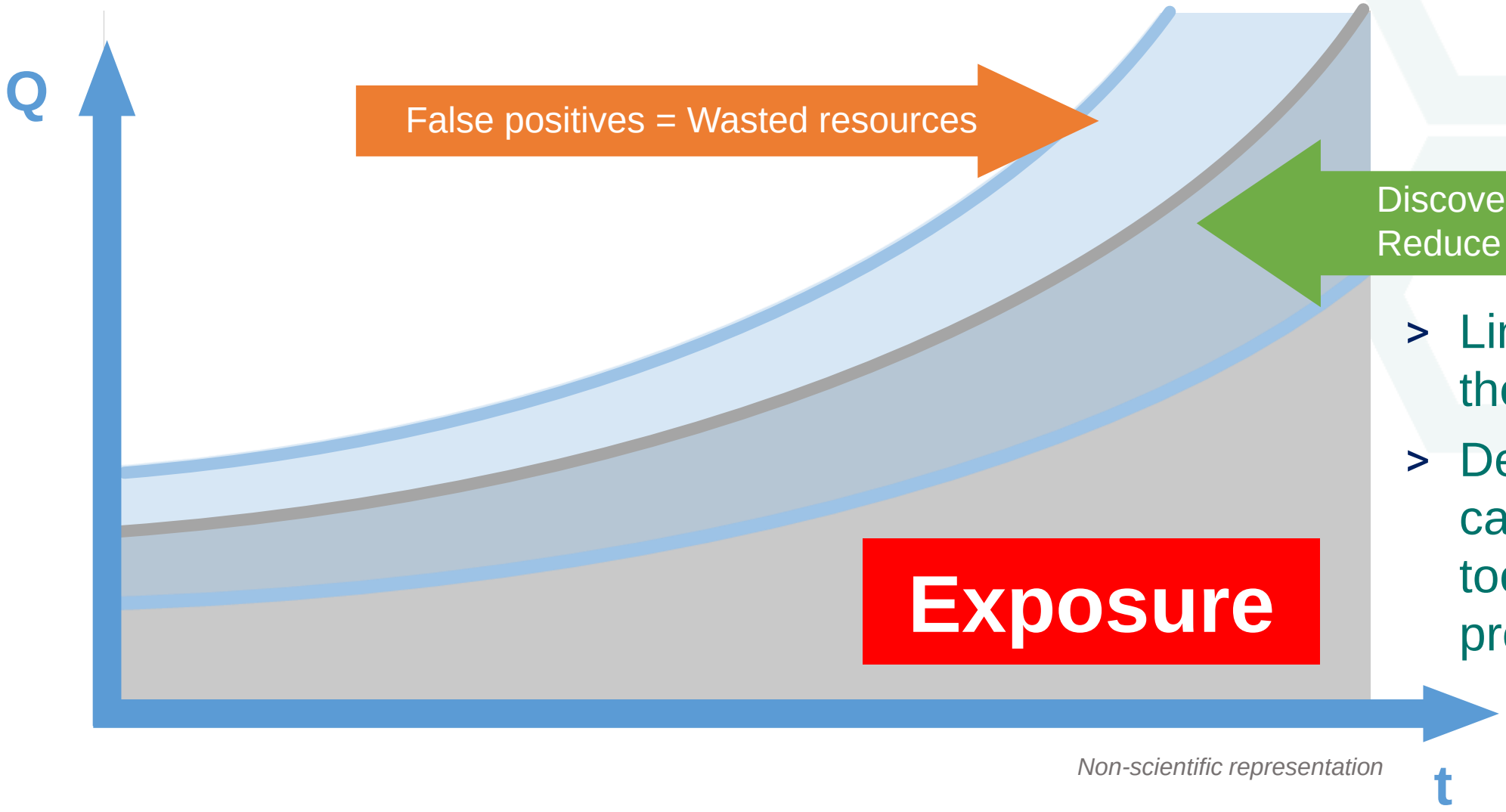
- Application complexity
- Vulnerabilities interplay

No security assessment



Non-scientific representation

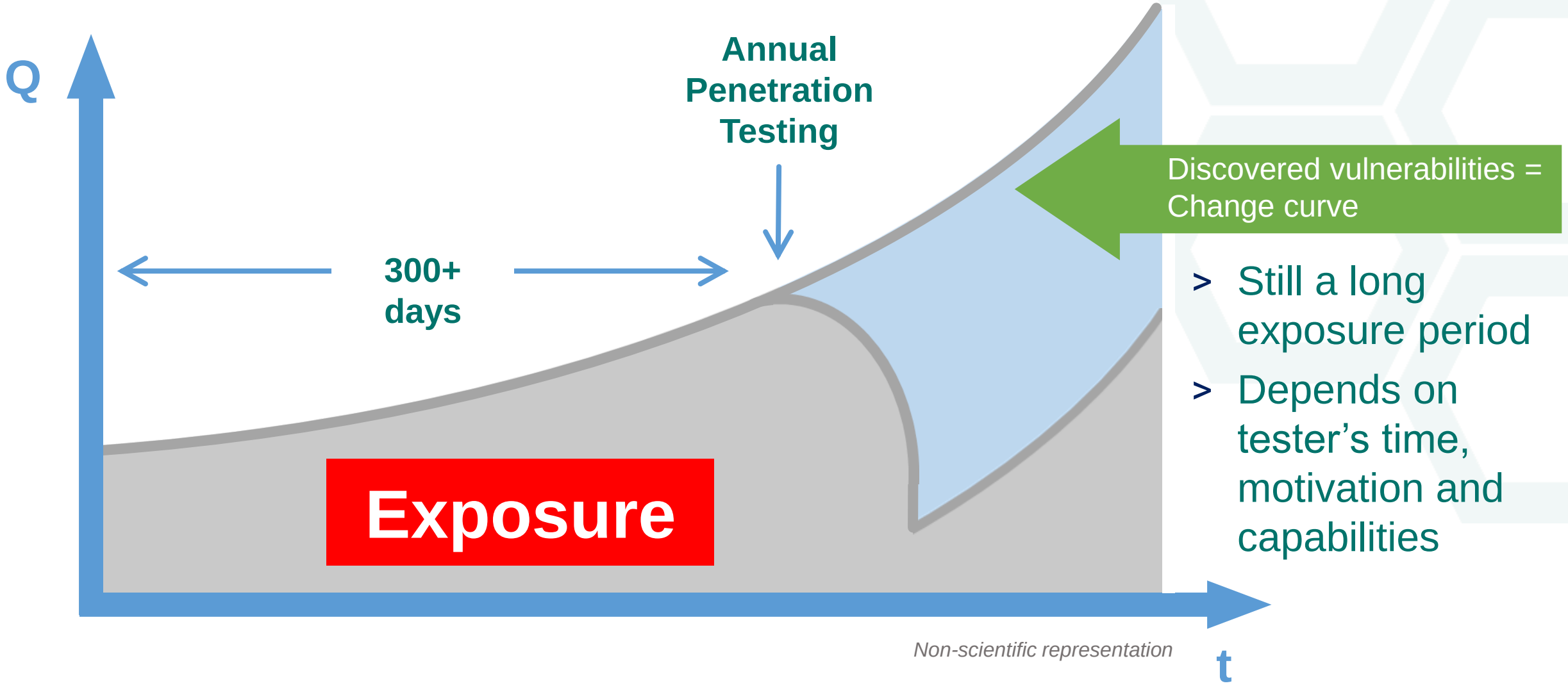
Using vulnerability scanning tools



Non-scientific representation

- Limited impact on the curve gradient
- Depends on capability of the tool, user and process

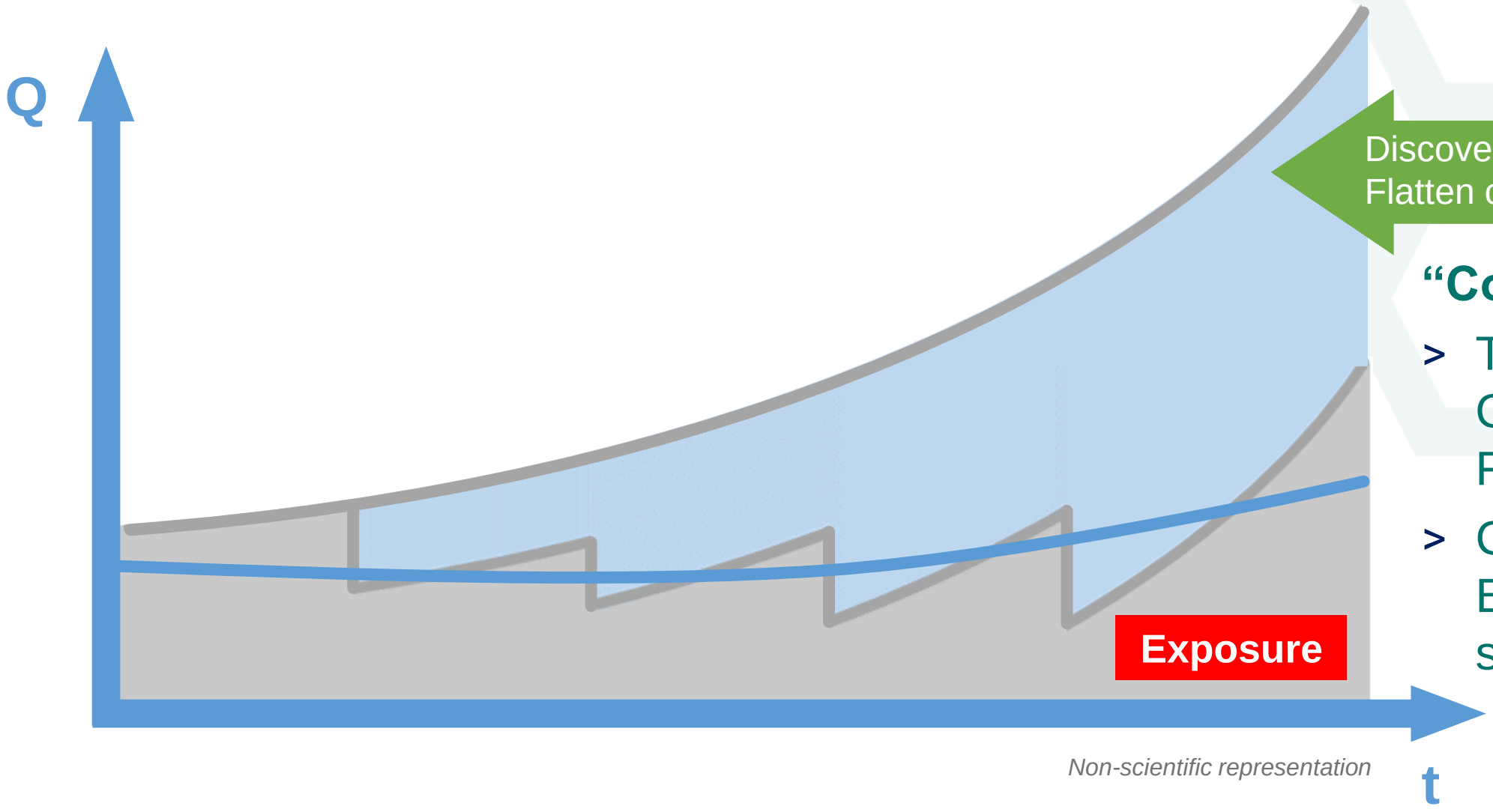
Is hacking yourself enough?



- Still a long exposure period
- Depends on tester's time, motivation and capabilities

Non-scientific representation

Doing it a lot more often

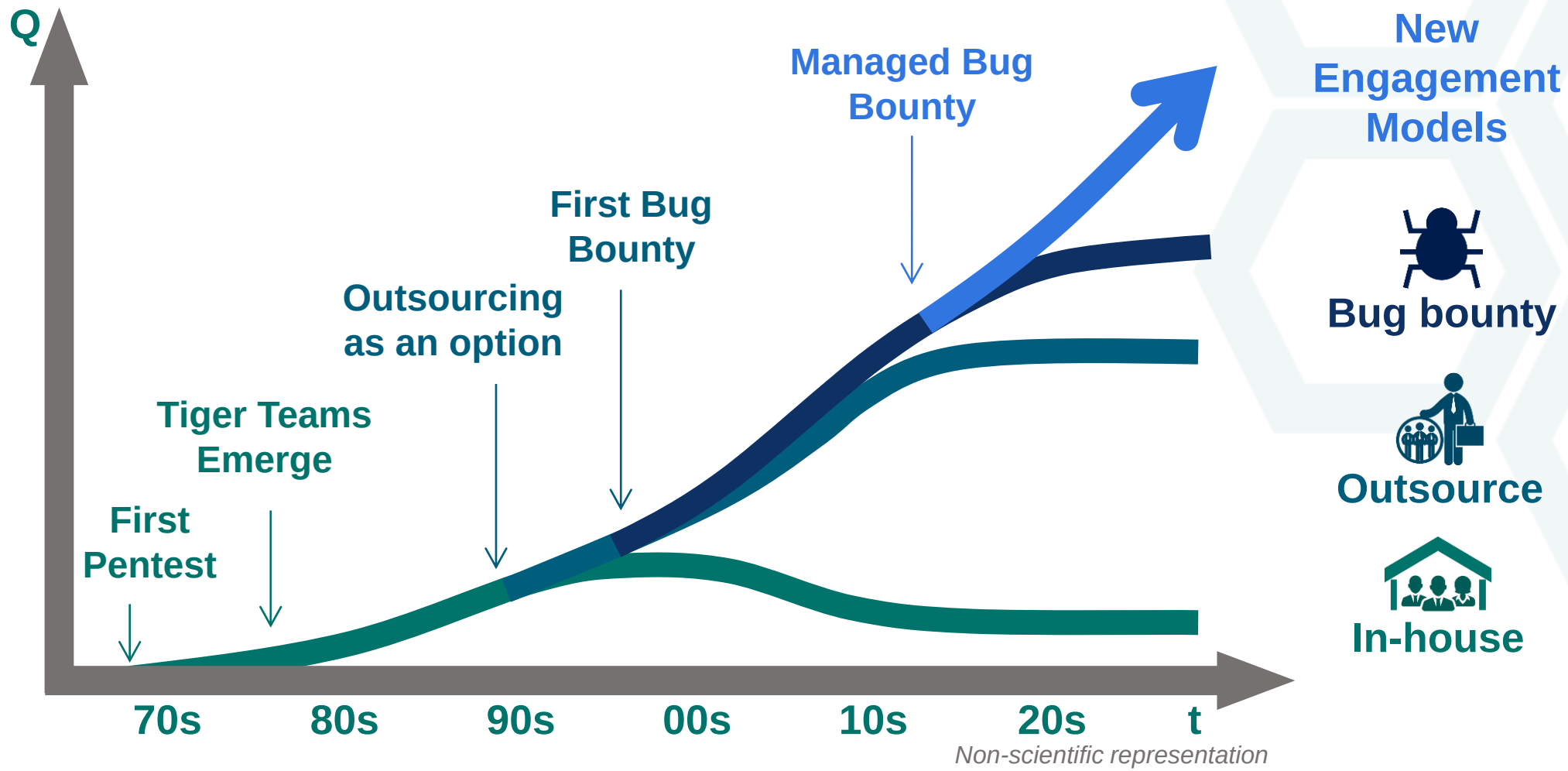


Non-scientific representation

“Continuous”?

- Test Early, Test Often, Test Forward?
- Constraint by Budget (staff, services spend)

How do we engage White Hats?



4 Prioritize controls based on real-world effectiveness against real-world attacks

a. Determine gaps based on selected framework, maturity assessment and required level (*remember: regulatory requirements*)

b. Prioritize implementation based on real-world effectiveness

ACSC Essential Eight

- Application whitelisting
- Patching applications
- Configuring Microsoft Office macro settings
- Application hardening
- Restricting admin privileges
- Patching operating systems
- Multi-factor authentication
- Daily backups

Originally published by the Australian Signals Directorate as the Top 4 Strategies that mitigates 85% of intrusions that the Australian Cyber Security Centre responds to.

5 Automate and orchestrate as far as possible

Automate: Use technology in place of manual processes (i.e. reduce dependency on qualified human resources)

Orchestrate: Integrate security tools, streamline processes and drive automation

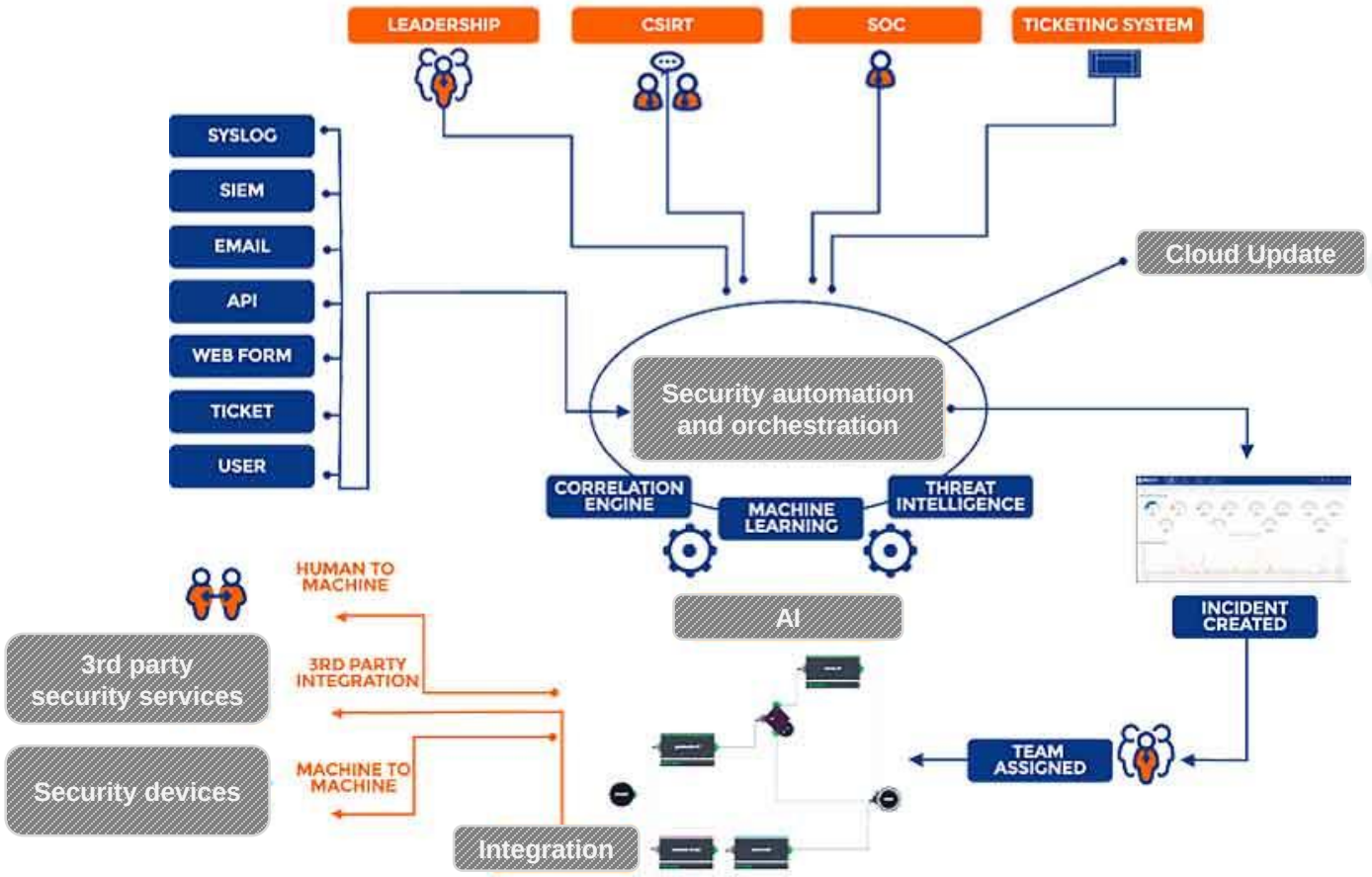
64% say increases productivity of security personnel

60% say helps address the volume of threats

54% say simplifies detection and response process

https://globenewswire.com/news-release/2018/06/26/1529520/0/en/Cybersecurity-Professionals-Face-Challenges-on-the-Path-to-Automation-Reveals-Juniper-Networks-and-Ponemon-Institute-Report.html

5 Automate and orchestrate as far as possible



My Tech Is Better Than Your Tech

SWARMNETICS

Some key trends

1. **Security testing at scale**

   Massive scanning to identify open ports (to communicate with systems) and testing of security vulnerabilities.

2. **Automatic vulnerability discovery and mitigation**

   Automatic defense (offense) systems that discover and fix (exploit) security vulnerabilities.

3. **Emergence of AI-driven arms race**

   Both defenders (anticipate and prevent attacks) and attackers (evade detection and increase success rates) are adopting the same technology.

Mass scanning the internet

MASSCAN: Mass IP Port Scanner

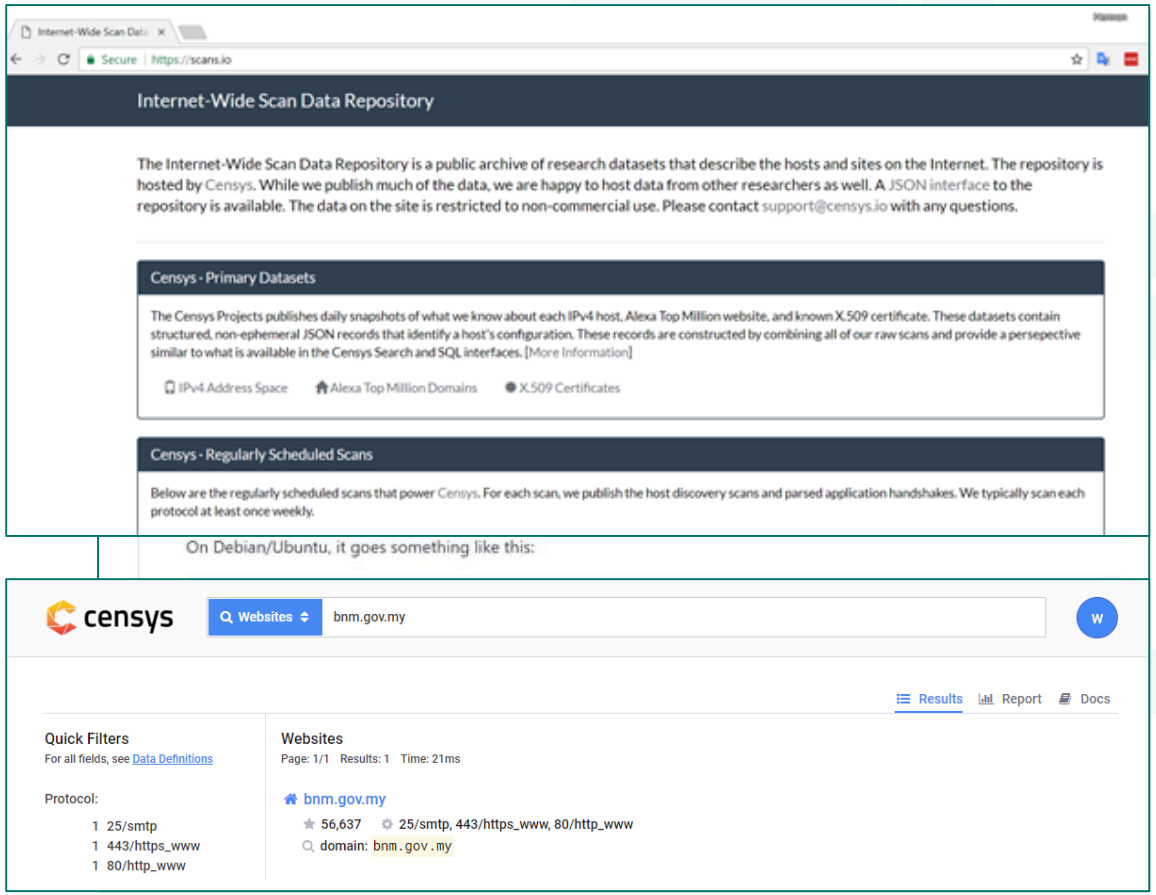
> Scans open ports

> Retrieves banners

> 6 minutes for the whole internet

Hosted by Censys – scans.io

> Regularly scans Alexa Top Million websites



Zerofox Experiment – Automated Phishing

- Extract data from Twitter users
- Use machine learning for profiling
- Send automated spear phishing tweets targeted at individual users

Phishing (mostly automated): 5-14% accuracy

Spear Phishing (highly manual): 45% accuracy

Zerofox (fully automated): 30% accuracy

https://www.blackhat.com/docs/us-16/materials/us-16-Seymour-Tully-Weaponizing-Data-Science-For-Social-Engineering-Automated-E2E-Spear-Phishing-On-Twitter.pdf

DARPA Cyber Grand Challenge 2016

- World's first **all-machine** cyber hacking tournament
- Each team created machines that autonomously defend their system and attack the opponent
- Each team is given a vulnerable system
- Each autonomous machine finds and patch vulnerable code in their system, and at the same time, attack their opponents' vulnerable systems before they are fixed

https://www.cybergrandchallenge.com

Generative Adversarial Network (GAN) Study

- Anti-malware solutions are using machine learning to detect new malware
- Malware authors try to attack the algorithm to look for ways to bypass
- Use machine learning algorithm (MalGAN) to generate malware examples that can bypass black-box machine learning based detection models – near zero detection rate

https://arxiv.org/abs/1702.05983

Bug bounties – Engaging the White Hats

- Programs where White Hats tries to find vulnerabilities by hacking a system
- White Hats are given monetary rewards or recognition (fame)
- Programs can be public or private
- Participants can be unlimited or by invite only

White Hat

An ethical hacker who specializes in penetration testing to find security vulnerabilities.

More than 600 Public Programmes Globally

Use of bug bounties for financial services

260 bugs since Mar 2015

198 bugs since Sep 2016

~1,000 bugs in 2014

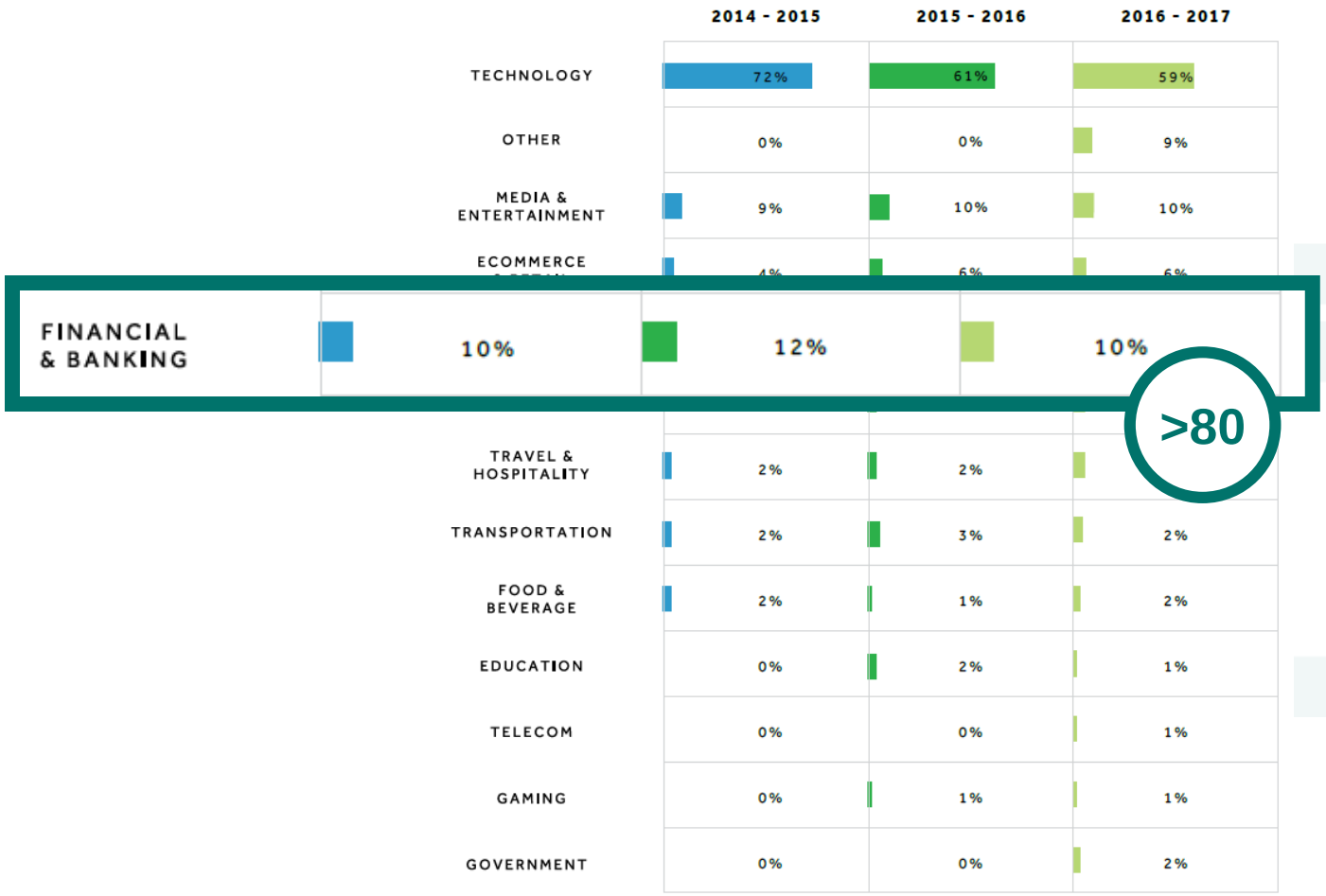


Figure 1: *Industries that launched programs from the overall share of programs, year over year.*

Q&A

Contact

weichieh@swarmnetics.com

+65 93828982

linkedin.com/in/weichieh

twitter.com/weichieh

SWARMNETICS

Eliminate All Vulnerabilities