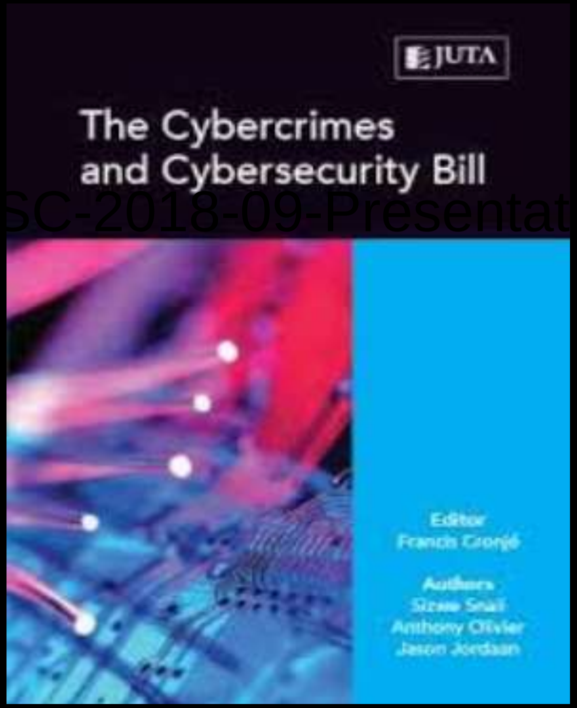
The Art of the Possible…

Information Sharing In the Globalizing Era of Cyber-Resilience, Contextualization & Orchestration

For acccess to IISC presentations, send email address to anyckt@ibm/com - Content::https://ibm.box.com/v/IISC-2018-09-Presentation



JUTA

The Cybercrimes and Cybersecurity Bill

Editor
Francis Cronjé

Authors
Sizwe Snail
Anthony Olivier
Jason Jordaan

SC-2018-09-Presentat s

Anyck Turgeon
CISO / Security & Cyber-Resilience Executive at IBM
12h

Law enforcement reduced by 60% DDoS (distributed denial-of-service) activities in Europe within days following the arrests of operators behind the hacking DDoS-for-hire website, Webstresser.org, in April. As "Crimeware-as-a-service" is one of the less profitable example of rising new economic segment called "platform criminality", revenues growth for this under-ground economy is noteworthy reaching $1.5 trillion annually including: 50% in illicit and illegal markets sales, 35% trade secrets and IP theft , 11% stolen data trading, less than 1% in "crimeware as a service" and less than 1% in ransomware. Prepare for the worst by starting your cyber-resilience plan today! More: https://lnkd.in/egHSffE) #DDoS #cyberresilience #cybersecurity

https://www.linkedin.com/in/anyckturgeon/
https://twitter.com/AnyckTurgeon

Anyck Turgeon – anyckt@ibm.com September 2018

Outstanding progress

“Cyber-threat intelligence ecosystem: a shopping center of ISAOs”

“Over 50 US ISAOs sharing cyber-intelligence”

“Automated (1-5 levels) Cyber-Security Information Sharing”

“Leveraging Traffic Light Protocol (TLP) for multi-tier exchanges”

“Use of STIX (Structured Threat Information Exchange) language & framework”

“The seed for global cyber-diplomacy”

The Art of the possible: It has been done…

"ONE OF THE COOLEST MOVIES OF THE YEAR" ★★★★
"SUPERB. A BLOCKBUSTER WITH BRAINS" ★★★★
NICOLAS CAGE
LORD OF WAR
HÄNDLER DES TODES
JARED LETO BRIDGET MOYNAHAN IAN HOLM and ETHAN HAWKE

Global Collaboration

IoT Contextualization

AI + Quantum =

The need for speed

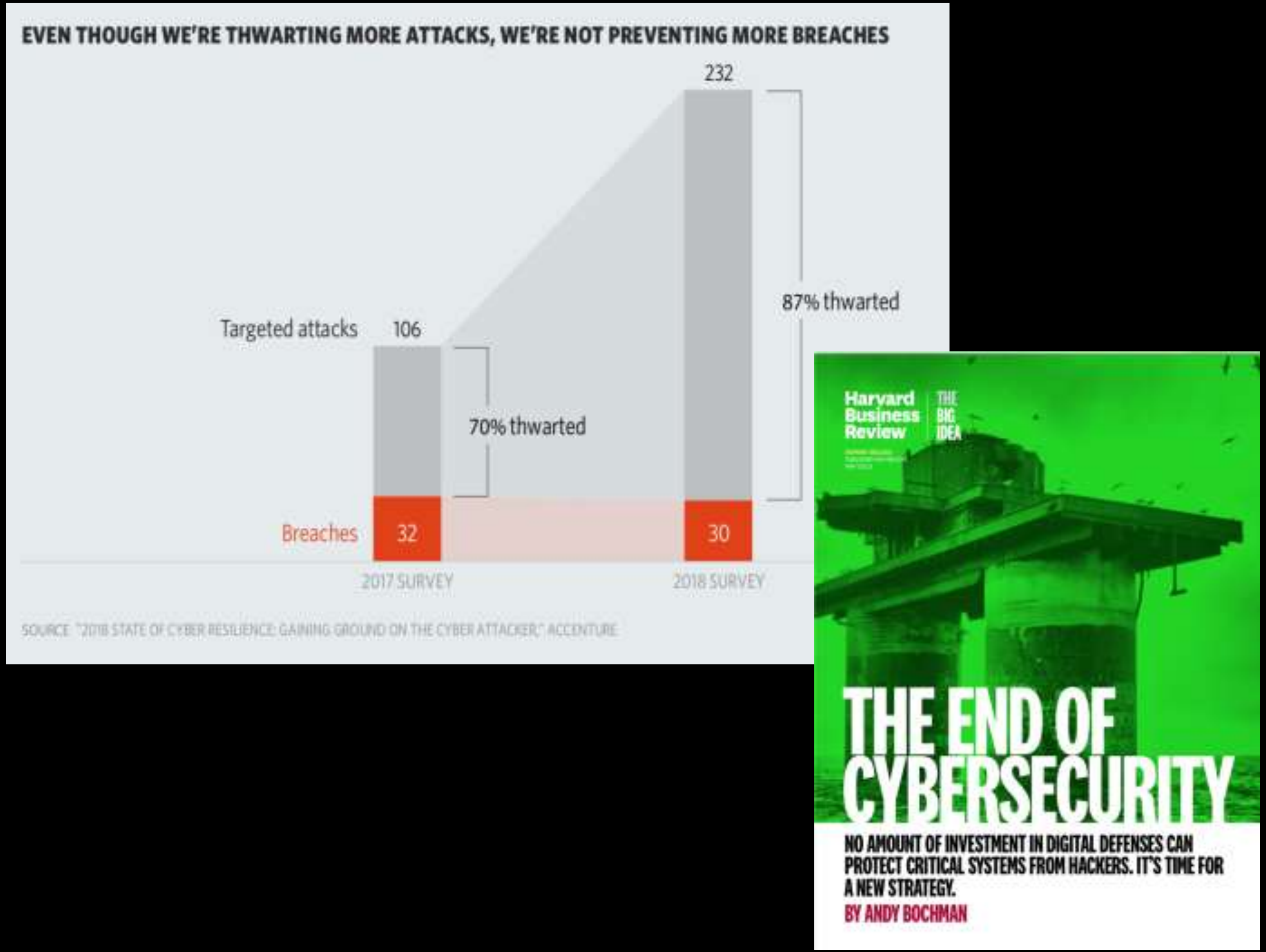
Un-biaised

Cyber Profiling

(United Clear & Dark Web)

What is Next: Innovating Information Sharing

To live is to suffer.
To survive is to find some meaning in the suffering.
Friedrich Nietzsche



SOURCE "2018 STATE OF CYBER RESILIENCE: GAINING GROUND ON THE CYBER ATTACKER," ACCENTURE

We choose to thrive by :

1) Prioritizing **Cyber-Resilience**

2) Zooming analysis with **AI & Quantum Contextualization** of cyber-intelligence

3) Delivering unprecedented outcomes with **Orchestration**

The Art of the Possible

Stop firing the fireman

Empower information sharing starting with cyber-resilience

Before and After

Cyber-Resilience

There are millions of ways to cyber-attack an organization today.

Large organizations already face billions of attacks per day.

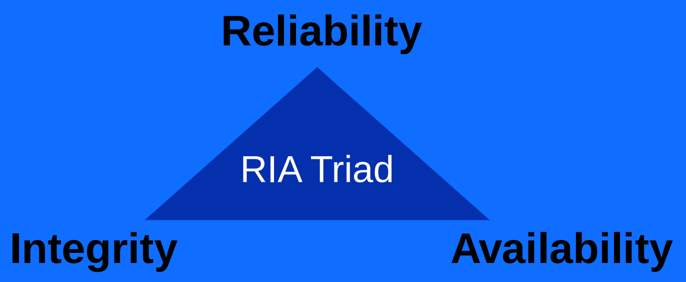
By 2020, we will have to deal with trillions of cyber-events daily.

Most organizations are already plagued by insider threats.

How to improve our response to global cyber-BOOMs?

Why Cyber Resilience? The “Always-On” Client Demand / Expectation

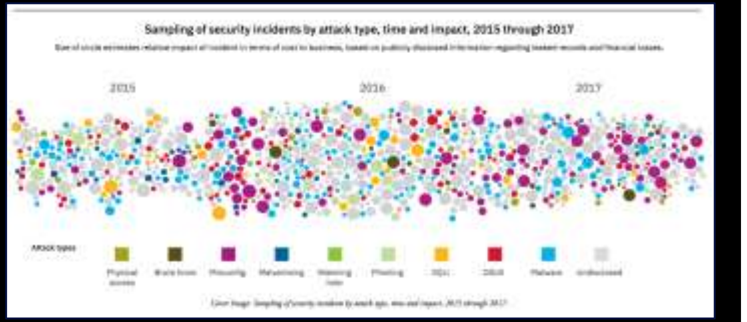
Cyber Resilience is an organization’s ability to continue delivering the intended outcomes despite adverse cyber incidents.



IBM Cyber Resilience =
Security + Resiliency + Networking solutions

Top 5 Threats of 2018[1]:

1. Cyber attack
2. Data breach
3. Unplanned IT outage
4. Interruptions to utility supply
5. Adverse weather


Sampling of security incidents by attack type, time and impact, 2015 through 2017

Business impact of cyber attacks and data breaches is very high

- $3.86 million
  average cost of a data breach[1]
- $350.44 million
  average cost of a mega data breach[2]
- Damaged brand reputation, loss of trust

[1,2] Ponemon Institute 2018 Cost of Data Breach Study

Analysts predict increased attacks and higher security and DR spending

- 27.9% average probability of material breach in the next 24 months[1]
- $96 billion
  security spending in 2018[2]
- $12.5 billion
  DRaaS market by 2022[3]

[1] Ponemon Institute 2018 Cost of Data Breach Study
[2] Gartner
[3] Markets and Markets

Cyber Risk is a C-Suite Priority:

- New worry for CEO, CIO and CISO: A career-ending cyberattack
- Mitigating cyber risks is now a top boardroom agenda[1]

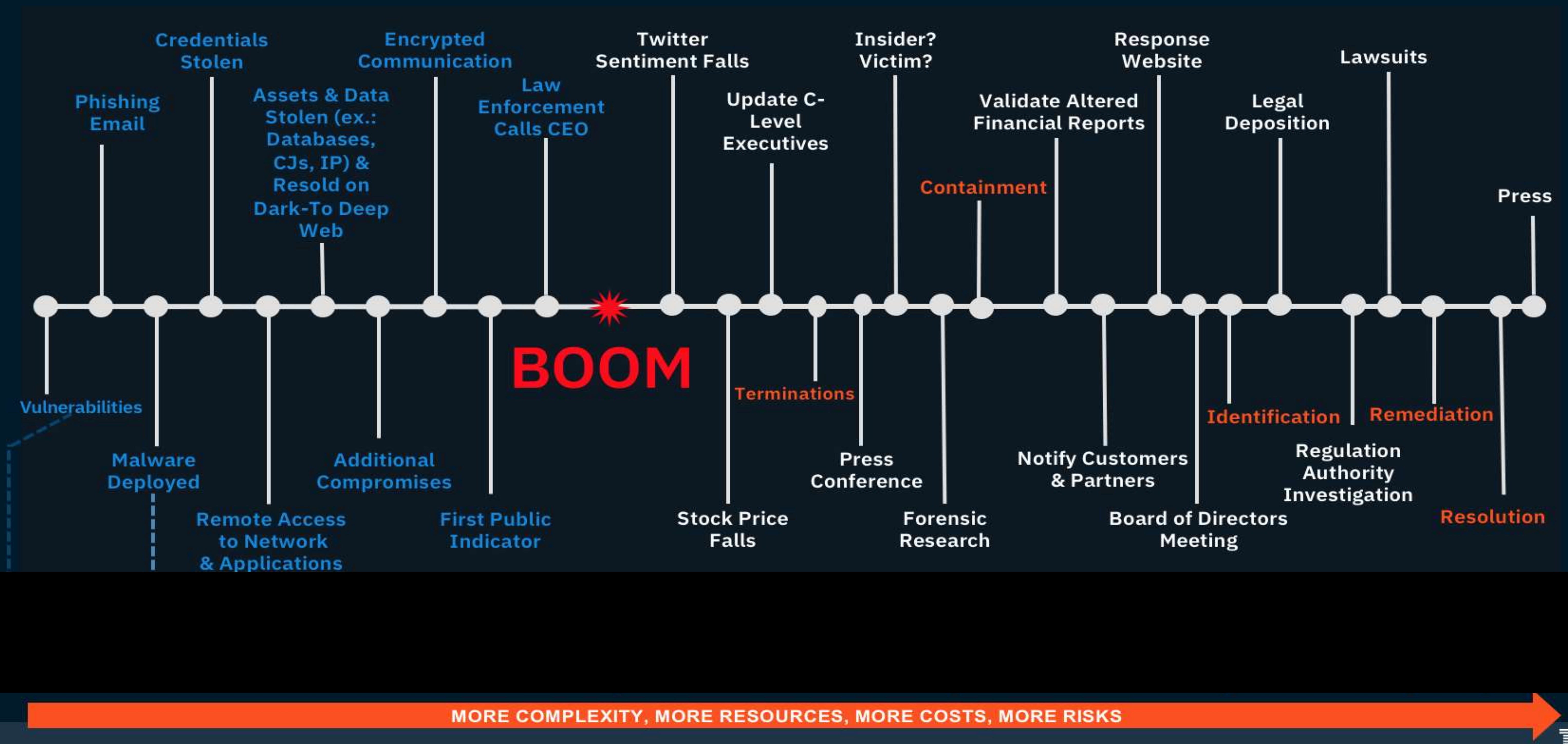
Regulations/Standards/Guidance:

- GDPR – Article 32
- ISAO 600-1
- 2015 US Presidential Executive Order 13691
- CPMI-IOSCO (Payments and Market Infrastructures)
- ISOs: ISO27001 (ISMS), ISO22301(BCMS), ISO27031 (comms)
- Sheltered Harbor – Appendix J
- MAS - Notice on Technology Risk Management

Key Client Challenges:

- Inability to fully comprehend rapidly evolving cyber risks landscape
- Inadequate incident response and DR plan
- Critical applications aren’t covered by DR programs

Today's Cyber-Incident Timeline



Vulnerabilities

Phishing Email

Malware Deployed

Credentials Stolen

Remote Access to Network & Applications

Assets & Data Stolen (ex.: Databases, CJs, IP) & Resold on Dark-To Deep Web

Additional Compromises

Encrypted Communication

First Public Indicator

Law Enforcement Calls CEO

BOOM

Twitter Sentiment Falls

Stock Price Falls

Update C-Level Executives

Terminations

Press Conference

Insider? Victim?

Forensic Research

Containment

Validate Altered Financial Reports

Notify Customers & Partners

Response Website

Board of Directors Meeting

Identification

Legal Deposition

Regulation Authority Investigation

Lawsuits

Remediation

Resolution

Press

MORE COMPLEXITY, MORE RESOURCES, MORE COSTS, MORE RISKS

Cyber-Security Today - “As Is” Experience

Did you know…
70% of ransomware business victims paid to get their data back
50% paid more than $10,000
20% paid more than $40,000.

SOURCE: IBM Study - Ransomware: How Consumers and Businesses Value Their Data

Michael

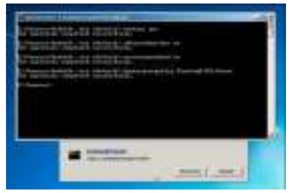
Chief Information Security Officer (CISO)

Client has insufficient tools, budget & resources to prevent cyber attacks.

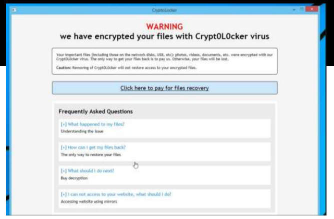
RYT hospital

Octopus tree

A cyber attack occurs when the cyber-criminal creates a contagious website. The viewer may receive a phishing email offering great promotions, find the site from a Google search or get rerouted from a valid site to the new bogus IP address.



When the user views the routed website, cocktail malware (including ransomware virus infection) is installed on the client’s system. Key logger is also often installed to obtain user credentials



CryptoLocker

WARNING
we have encrypted your files with Crypt0L0cker virus

Your important files (including those on the network disks, USB, etc): photos, videos, documents, etc. were encrypted with our Crypt0L0cker virus. The only way to get your files back is to pay us. Otherwise, your files will be lost.

Caution: Removing of Crypt0L0cker will not restore access to your encrypted files.

Click here to pay for files recovery

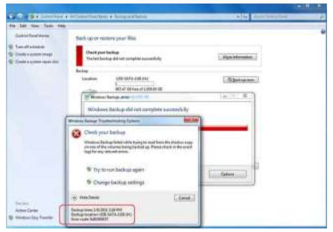
Frequently Asked Questions

[+] What happened to my files?
Understanding the issue

[+] How can I get my files back?
The only way to restore your files

[+] What should I do next?
Buy decryption

[+] I can not access to your website, what should I do?
Accessing website using mirrors

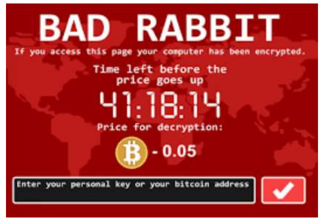


Ransomware takes a copy of the valid data while it encrypts production filesystem and latest backup copy.

Key logger captures valid user credentials.

Other malware gets installed at different intervals

Is this really a solution?



BAD RABBIT

If you access this page your computer has been encrypted.

Time left before the price goes up

41:18:14

Price for decryption:

- 0.05

Enter your personal key or your bitcoin address

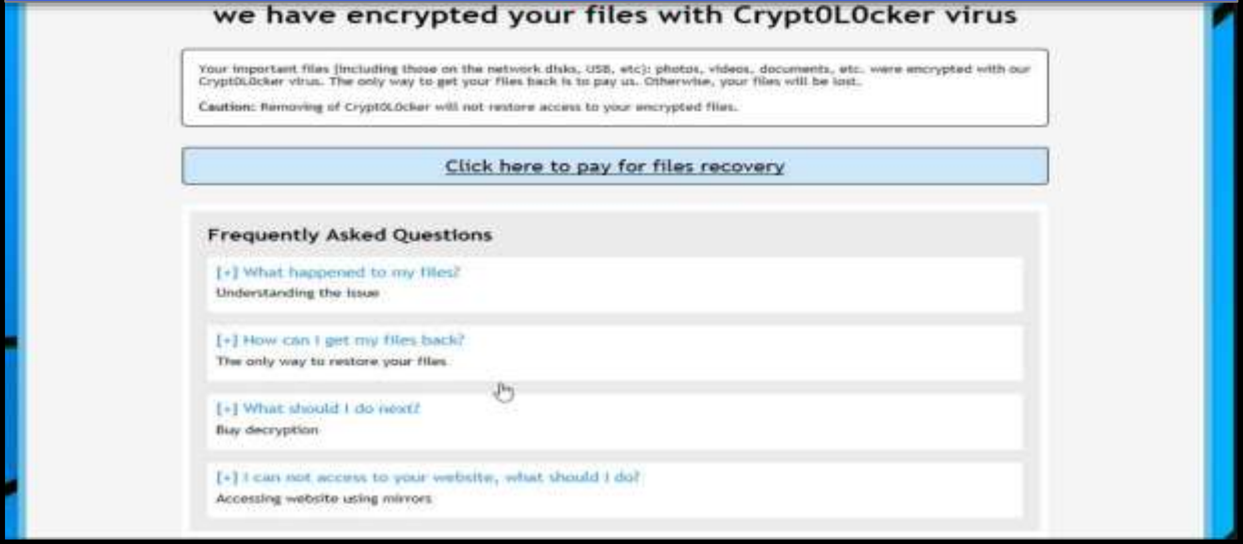
Client receives ransomware notice with terms of payment and panics. Initial terms of payment are more affordable (ex: pay $1,000 within 30 minutes.)

Client chooses to pay ransom via bitcoin to unlock production system data and MAY receive unencrypted file back.

Cyber-criminals sell valid credentials, data, etc. on the dark web for others to attack successfully & re-attacks organization later after being done with crypto-mining

Cyber Security – “As Is” Failure is Becoming Exponentially More Costly…

Since 2016, Angler generates $34 Million / month



we have encrypted your files with Crypt0L0cker virus

Your important files (including those on the network disks, USB, etc): photos, videos, documents, etc. were encrypted with our Crypt0L0cker virus. The only way to get your files back is to pay us. Otherwise, your files will be lost.

Caution: Removing of Crypt0L0cker will not restore access to your encrypted files.

Click here to pay for files recovery

Frequently Asked Questions

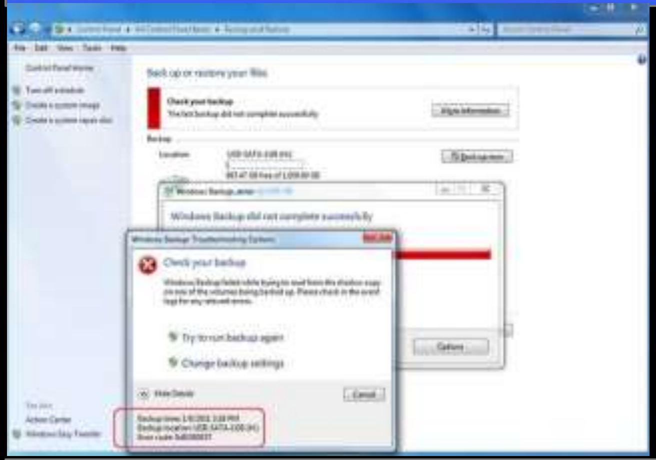
[+] What happened to my files?
Understanding the issue

[+] How can I get my files back?
The only way to restore your files

[+] What should I do next?
Buy decryption

[+] I can not access to your website, what should I do?
Accessing website using mirrors

Since 2017, Ransomware generates $40 Million /month



Back up or restore your files

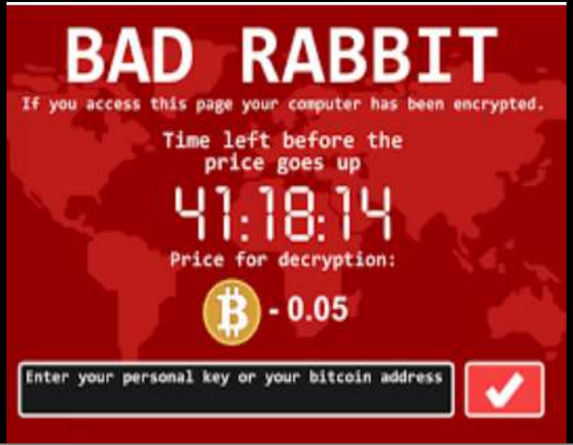
Check your backup
The last backup did not complete successfully

Windows Backup did not complete successfully

Check your backup

Try to run backup again

Change backup settings



BAD RABBIT

If you access this page your computer has been encrypted.

Time left before the price goes up

41:18:14

Price for decryption: ₿ - 0.05

Enter your personal key or your bitcoin address ✓

& is more exciting with Crypto-mining

Now, Modern Cocktail Malware is much more lucrative

WEEK 1	WEEK 2	WEEK 3	Week 4	Week AI
$10,000	**$1M**	**$10M**	**$100M**	**$10B**
1 hack	100 hacks	1,000 hacks	10,000 hacks	1M hacks

Cyber Security – “As Is” - Resulting Impacts & Business + IT Challenges

Unacceptable Business & Economic Impacts

Inefficient Point In Time copies Point in time copies provided by traditional backup has high RPO and RTO – **FAILING RECOVERY**

Recovery is too long and has frequent failures due to heavy manual operations. Becomes more challenging in Cyber Attacks – **FAILING BUSINESS & IT PERFORMANCE**

Testing disrupts organizations – **FAILING HIGH-AVAILABILITY**

Regulations impose new requirements FINRA Rule 4511, SEC Rule 17a-4, HIPAA, Data Protection Directive, GDPR, FFIEC Appendix J – **FAILING COMPLIANCE**

Continuous Network Exposure - Continuous network exposure can cause corruption propagation to the DR Sites, causing both primary and DR unusable – **FAILING SYSTEMS PROTECTION**

DR/ Backups Being Targeted Ransomware attacks corrupting DR & backup copies directly **– FAILING WITH INFECTED / INFECTING RECOVERY**

Outdated runbooks are common - Dynamic environments thwart application recovery activities - **FAILING RECOVERY * SECURITY (NO ORCHESTRATION)**

Slow Recovery of Business Services, post Cyber attack leads to **Unacceptable Business Impacts – FAILING BUSINESS SURVIVAL**

The “Evil Twins” Attack

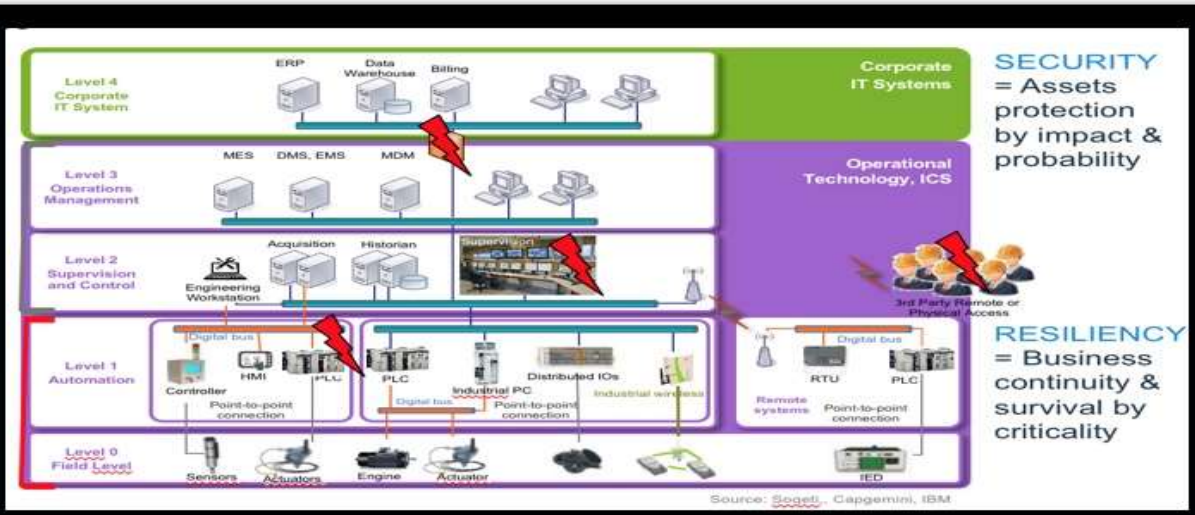
#1 World’s Most Lethal Cyber-Attack

TIMELINE:

Triton hackers had penetrated controller & safety systems	Triton attack detected with plant shutdown	Public & ICS-CERT disclosure	Awareness Campaign (s4x18)	New tools & solutions
June 2017	August 2017	December 2017	January 2018	March 2018+

- **Advanced**: Coordinated & expensive attack (1 man year+) gaining access & control of OT control & safety systems (levels 0 to 4 were impacted.
- **Intentionally Malicious**: Objective was NOT to shutdown the plant and was preformed by professional hackers that removed their trails.
- **Insider-Access**: Coordinated attack of separate devices with different access performed by Nation-State professionals
- **Impact:** Plant shutdown when tests of irregular commands in memory were detected.
- **Remaining threat**: 18,000 plants part of critical infrastructure globally are now vulnerable
- Heightened risks: from medium-high IT / cyber-risks to critically-lethal enterprise & global-risks

MORE: https://www.midnightbluelabs.com/blog/2018/1/16/analyzing-the-triton-industrial-malware

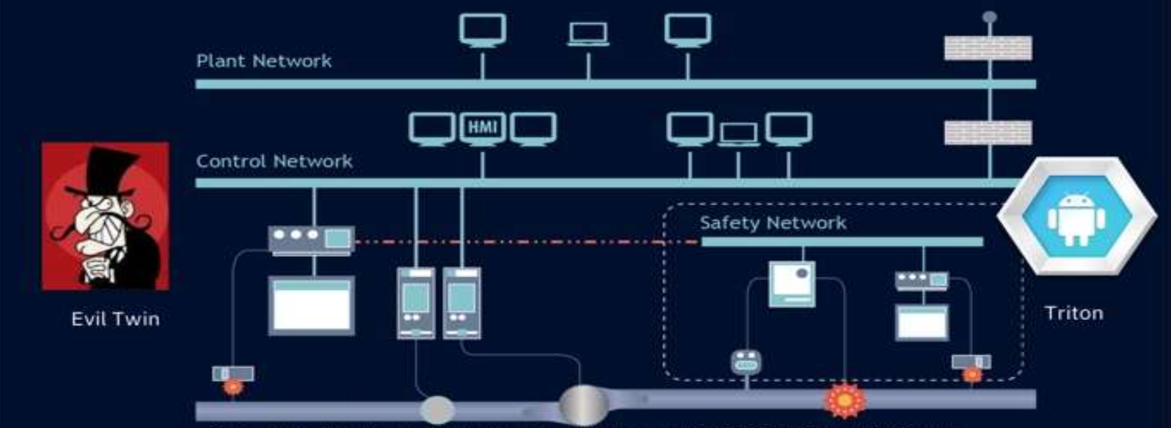


SECURITY = Assets protection by impact & probability

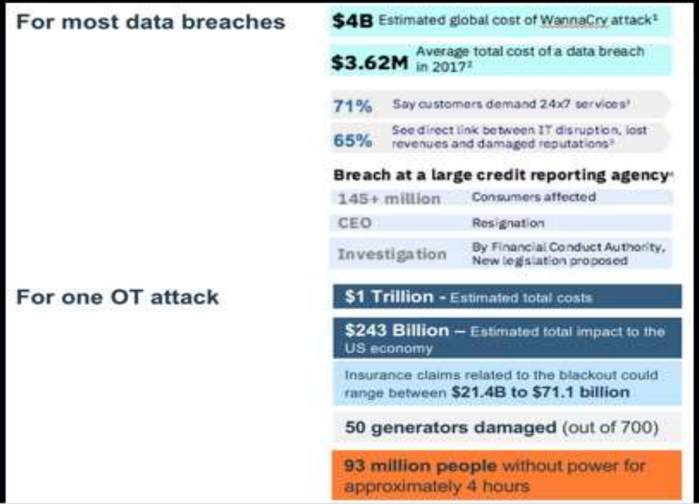
RESILIENCY = Business continuity & survival by criticality

Source: Sogeti., Capgemini, IBM

Simplified Control System Layout
The malware had to employ a “Twin” to raise damage @ critical level



Post provided by: Michael Assante, Director of Industrials and Infrastructure and SANS ICS & SCADA Lead at SANS Institute



For most data breaches

$4B Estimated global cost of WannaCry attack[1]

$3.62M Average total cost of a data breach in 2017[2]

71% Say customers demand 24x7 services[3]

65% See direct link between IT disruption, lost revenues and damaged reputations[3]

Breach at a large credit reporting agency[4]

145+ million	Consumers affected
CEO	Resignation
Investigation	By Financial Conduct Authority, New legislation proposed

For one OT attack

$1 Trillion - Estimated total costs

$243 Billion – Estimated total impact to the US economy

Insurance claims related to the blackout could range between **$21.4B to $71.1 billion**

50 generators damaged (out of 700)

93 million people without power for approximately 4 hours

+ **DEATHS** & long-term damages to the environment

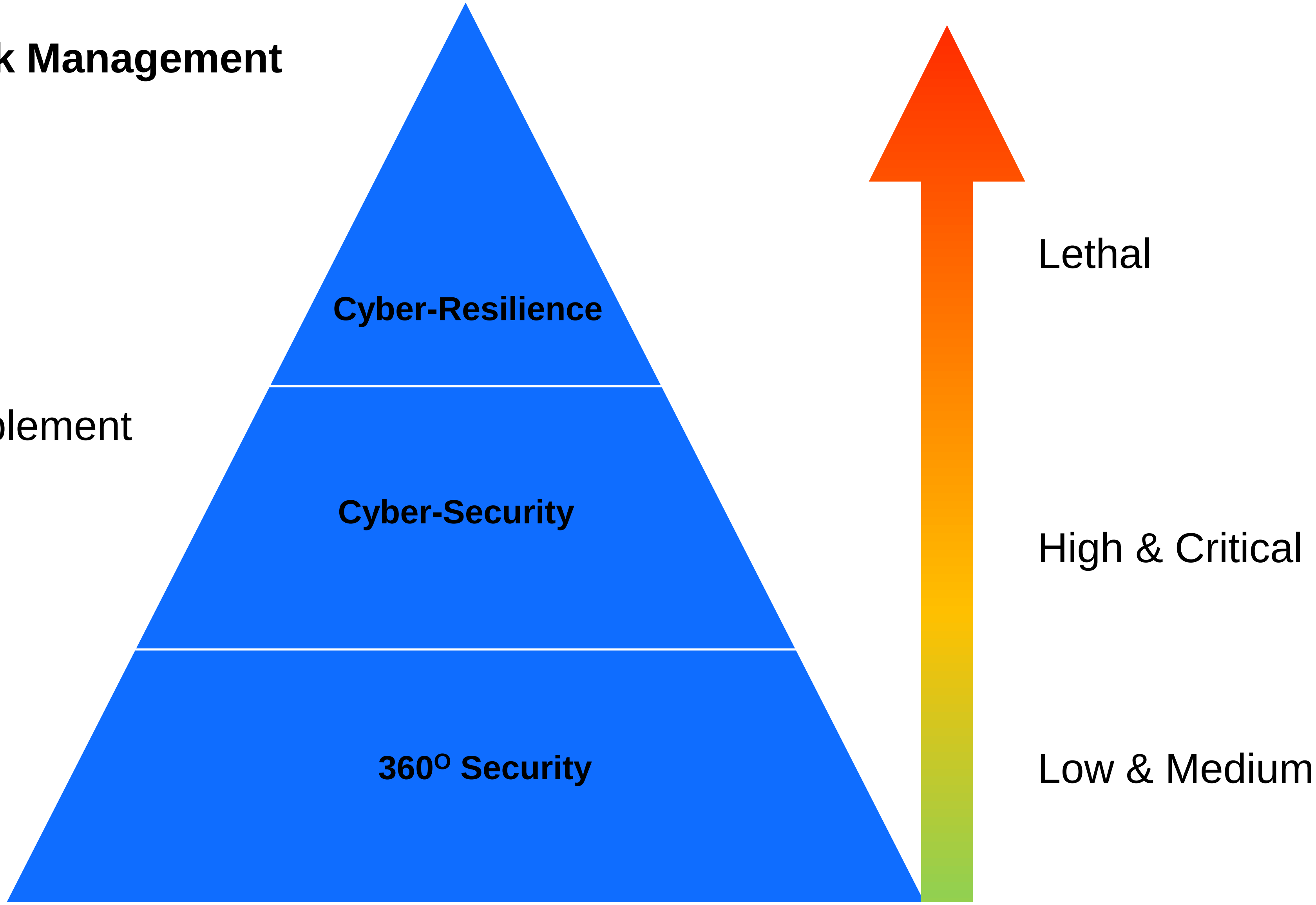
Innovating Information Sharing

Re-Asses & Re-Align with a **Dynamic** Enterprise **Risk Management**

(from 2 to 9+ AI sense-making / scaled dimensions)

Expand to **Global Exchanges**

Gain near **Real-Time Speed** with AI & Quantum enablement



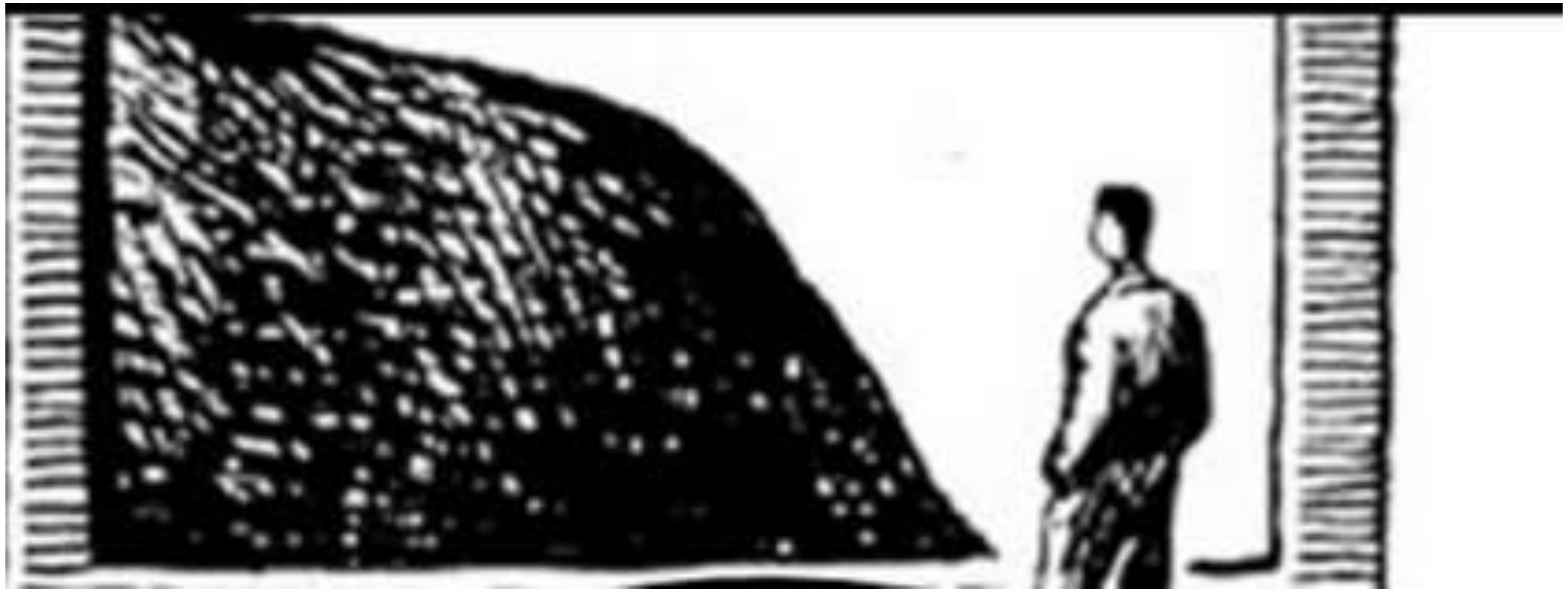
The Art of the Possible

Contextualization

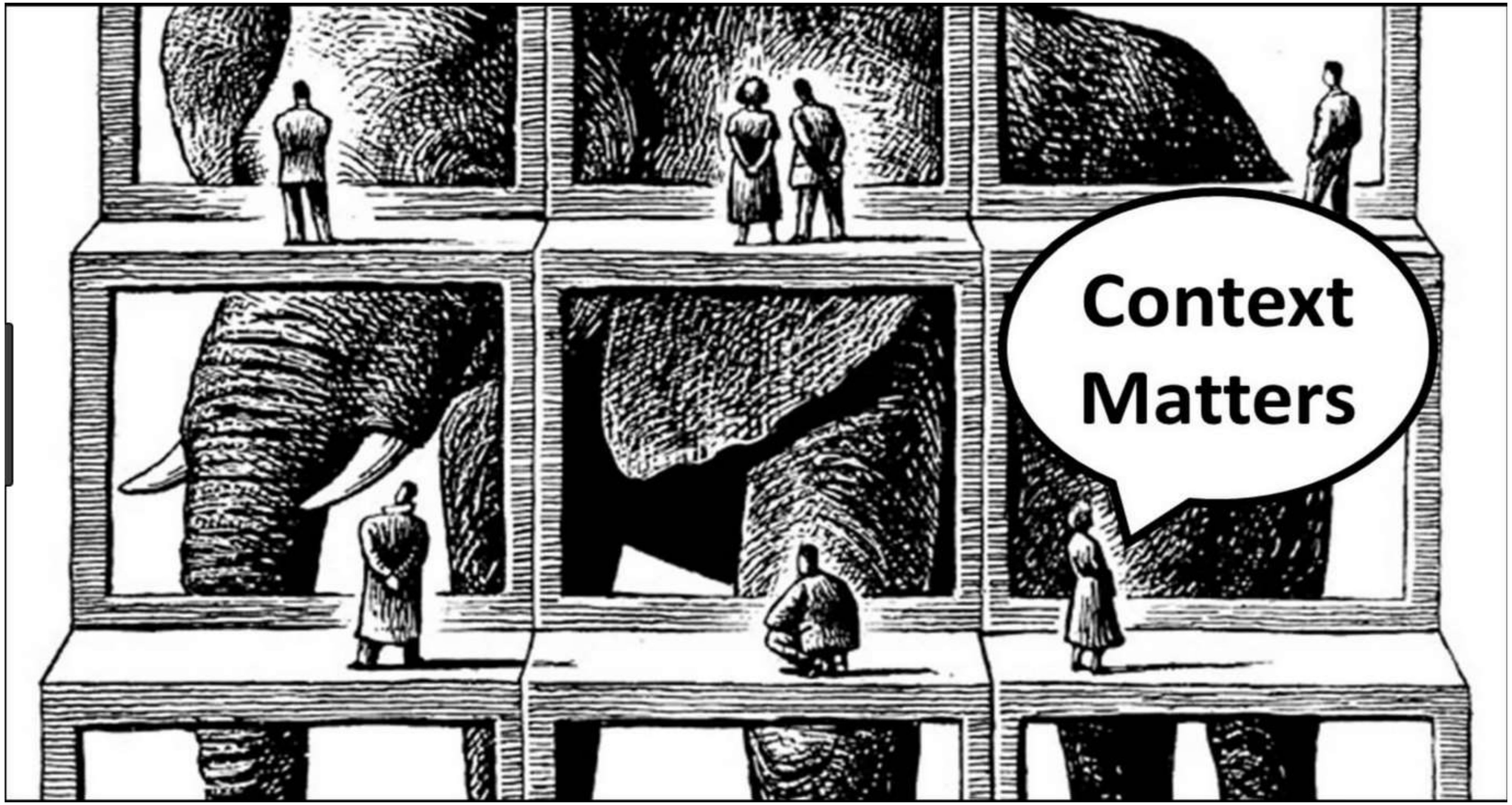
Innovating Information Sharing with Contextualization

Do you get a fuzzy feeling when you are reviewing shared information?

- Unsure / Non-conclusive
- Feeling incomplete
- Not actionable



Innovating Information Sharing with Graded Contextualization



GRADE YOUR CONTEXTUALIZED INFORMATION

- What information will incite action?

- Can you gain information that meets “beyond reasonable doubt?”

- How do you expand to trusted holistic information?

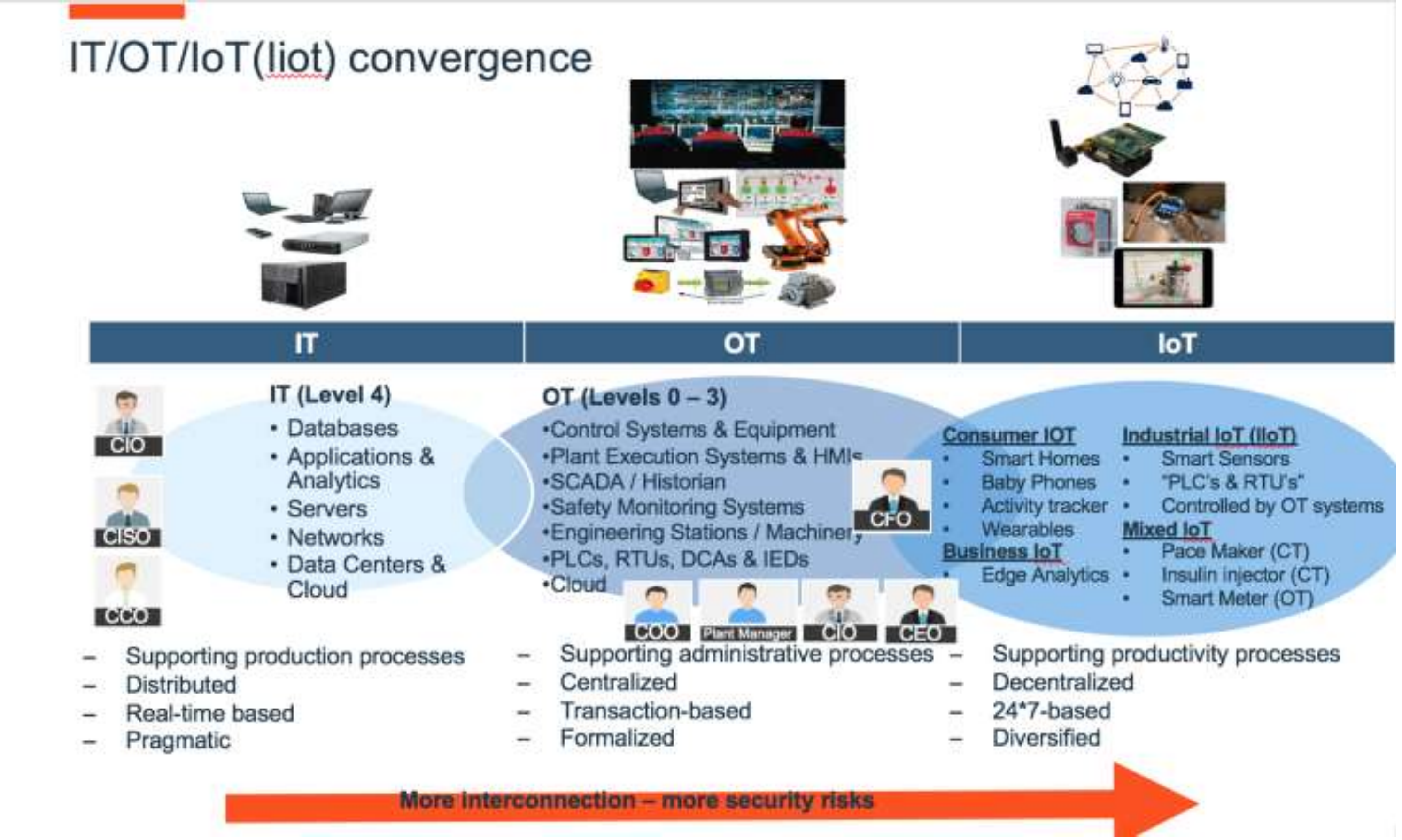
Innovating Information Sharing with Complete Contextualization

Let’s get to global exchanges

What degree of contextualization do you need to provide?

Innovating Information Sharing with Complete Contextualization

Plan for various degrees of holistic cyber-resilience, cyber-security & 360º security information sharing



IT/OT/IoT(Iiot) convergence

IT	OT	IoT

IT (Level 4)
- Databases
- Applications & Analytics
- Servers
- Networks
- Data Centers & Cloud

OT (Levels 0 – 3)
- Control Systems & Equipment
- Plant Execution Systems & HMIs
- SCADA / Historian
- Safety Monitoring Systems
- Engineering Stations / Machinery
- PLCs, RTUs, DCAs & IEDs
- Cloud

Consumer IOT
- Smart Homes
- Baby Phones
- Activity tracker
- Wearables

Business IoT
- Edge Analytics

Industrial IoT (IIoT)
- Smart Sensors
- "PLC's & RTU's"
- Controlled by OT systems

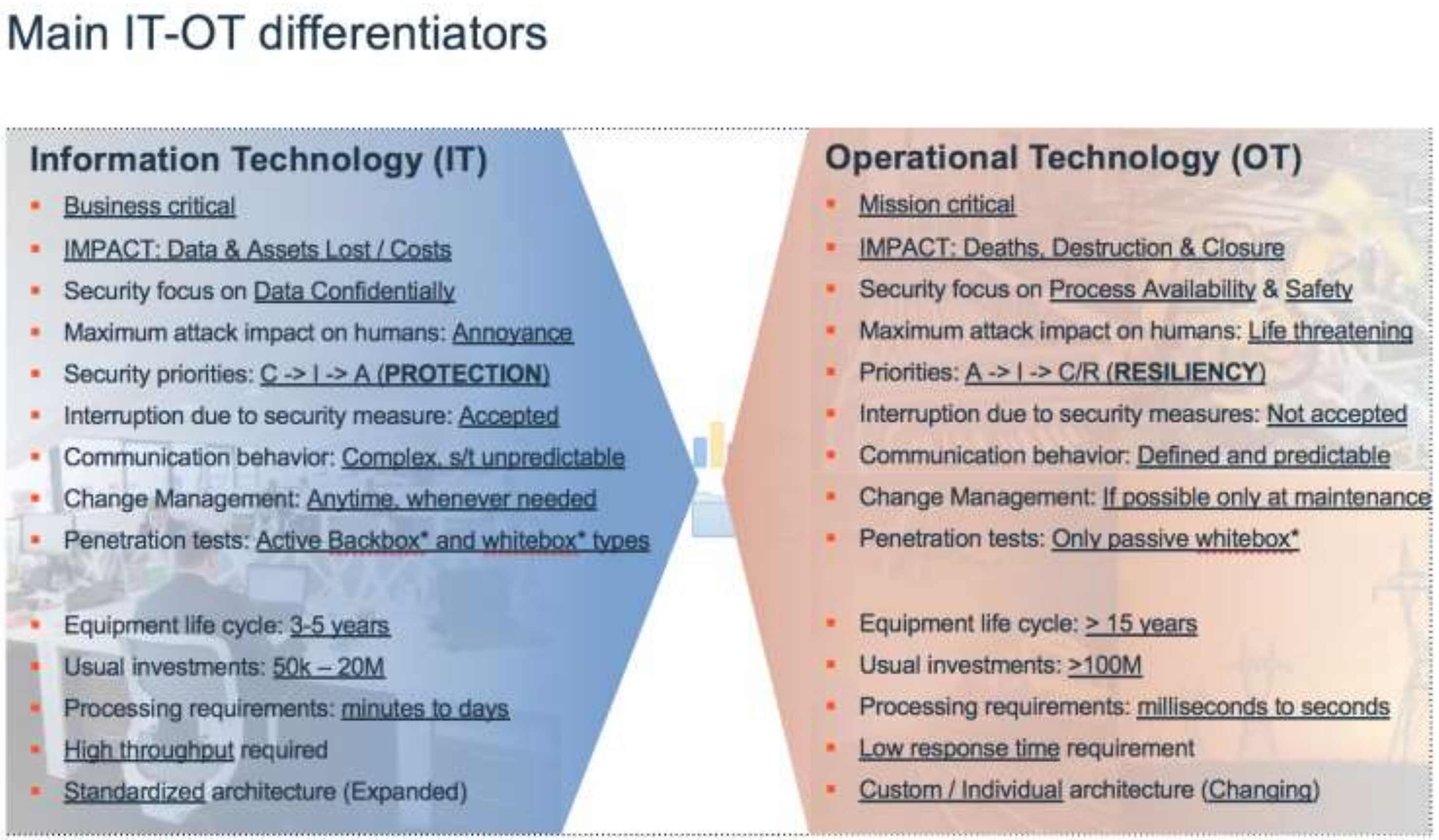
Mixed IoT
- Pace Maker (CT)
- Insulin injector (CT)
- Smart Meter (OT)

- Supporting production processes
- Distributed
- Real-time based
- Pragmatic

- Supporting administrative processes
- Centralized
- Transaction-based
- Formalized

- Supporting productivity processes
- Decentralized
- 24*7-based
- Diversified

More interconnection – more security risks



Main IT-OT differentiators

Information Technology (IT)
- Business critical
- IMPACT: Data & Assets Lost / Costs
- Security focus on Data Confidentially
- Maximum attack impact on humans: Annoyance
- Security priorities: C -> I -> A (PROTECTION)
- Interruption due to security measure: Accepted
- Communication behavior: Complex, s/t unpredictable
- Change Management: Anytime, whenever needed
- Penetration tests: Active Backbox* and whitebox* types

- Equipment life cycle: 3-5 years
- Usual investments: 50k – 20M
- Processing requirements: minutes to days
- High throughput required
- Standardized architecture (Expanded)

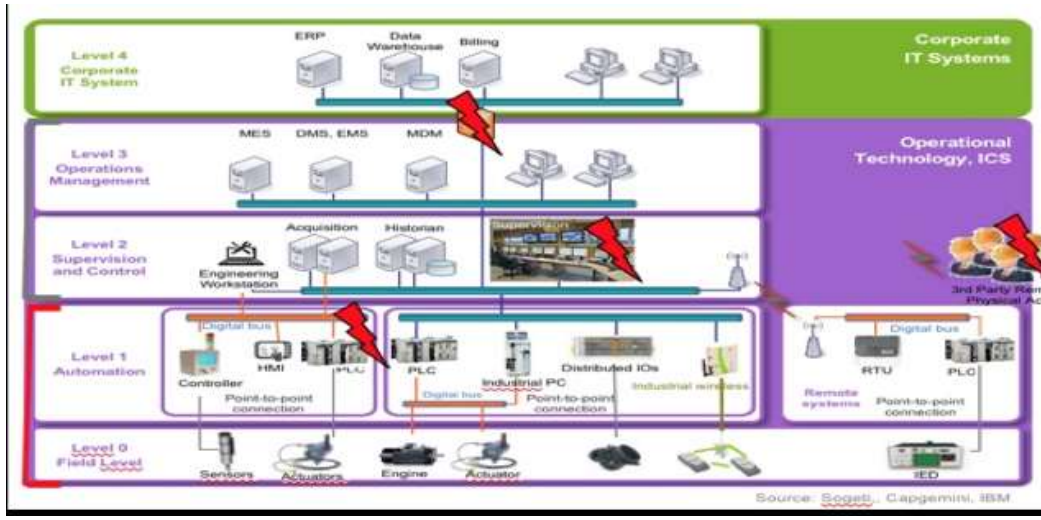
Operational Technology (OT)
- Mission critical
- IMPACT: Deaths, Destruction & Closure
- Security focus on Process Availability & Safety
- Maximum attack impact on humans: Life threatening
- Priorities: A -> I -> C/R (RESILIENCY)
- Interruption due to security measures: Not accepted
- Communication behavior: Defined and predictable
- Change Management: If possible only at maintenance
- Penetration tests: Only passive whitebox*

- Equipment life cycle: > 15 years
- Usual investments: >100M
- Processing requirements: milliseconds to seconds
- Low response time requirement
- Custom / Individual architecture (Changing)

Innovating Information Sharing with Reliable & Actionable Contextualization

Use intelligent automation for reconciliation

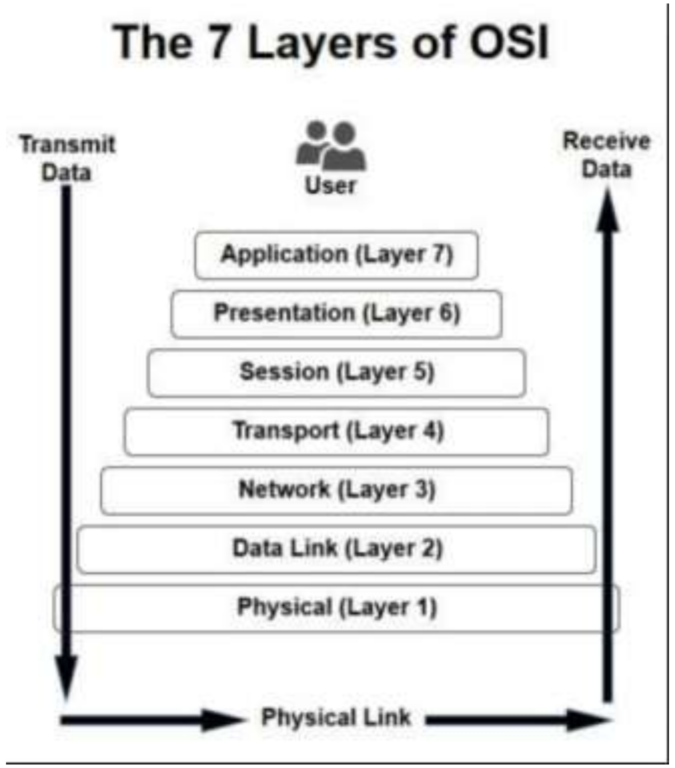
Intrinsically… for reliability (from 3+ independent sources)



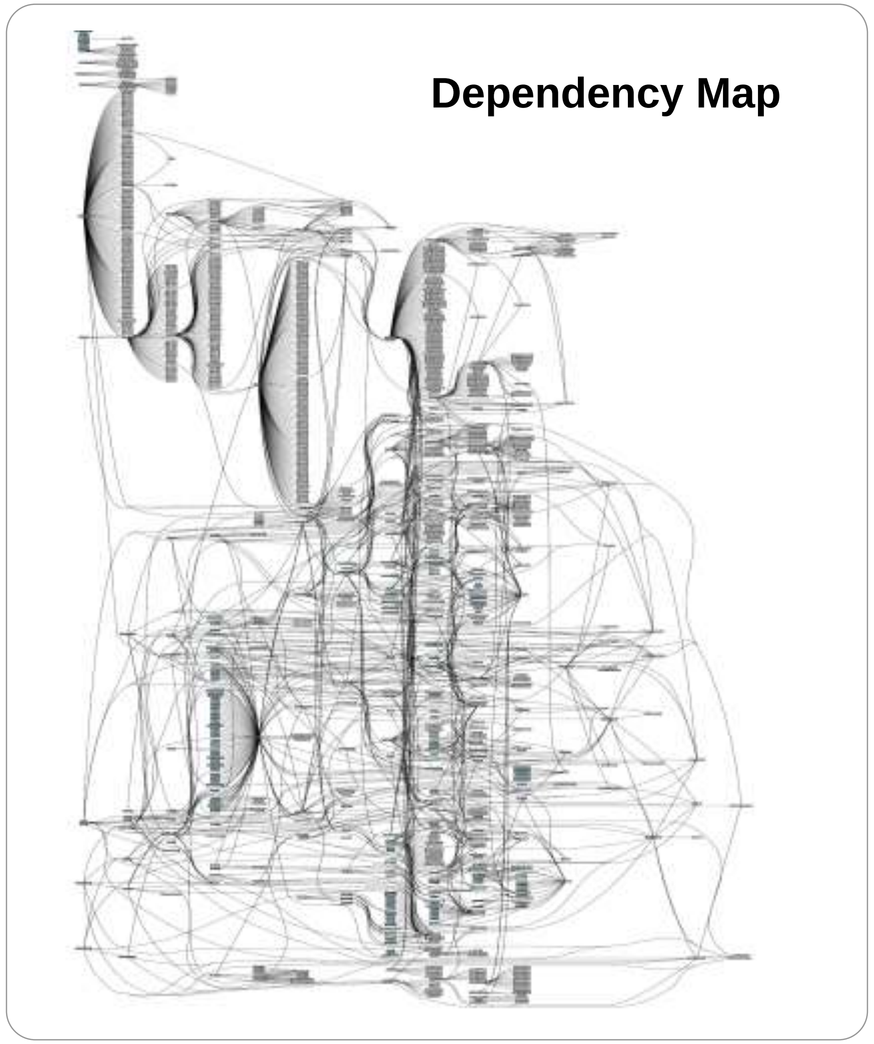
Source: Sogeti,, Capgemini, IBM

SECURITY = Assets protection by impact & probability

RESILIENCY = Business continuity & survival by criticality



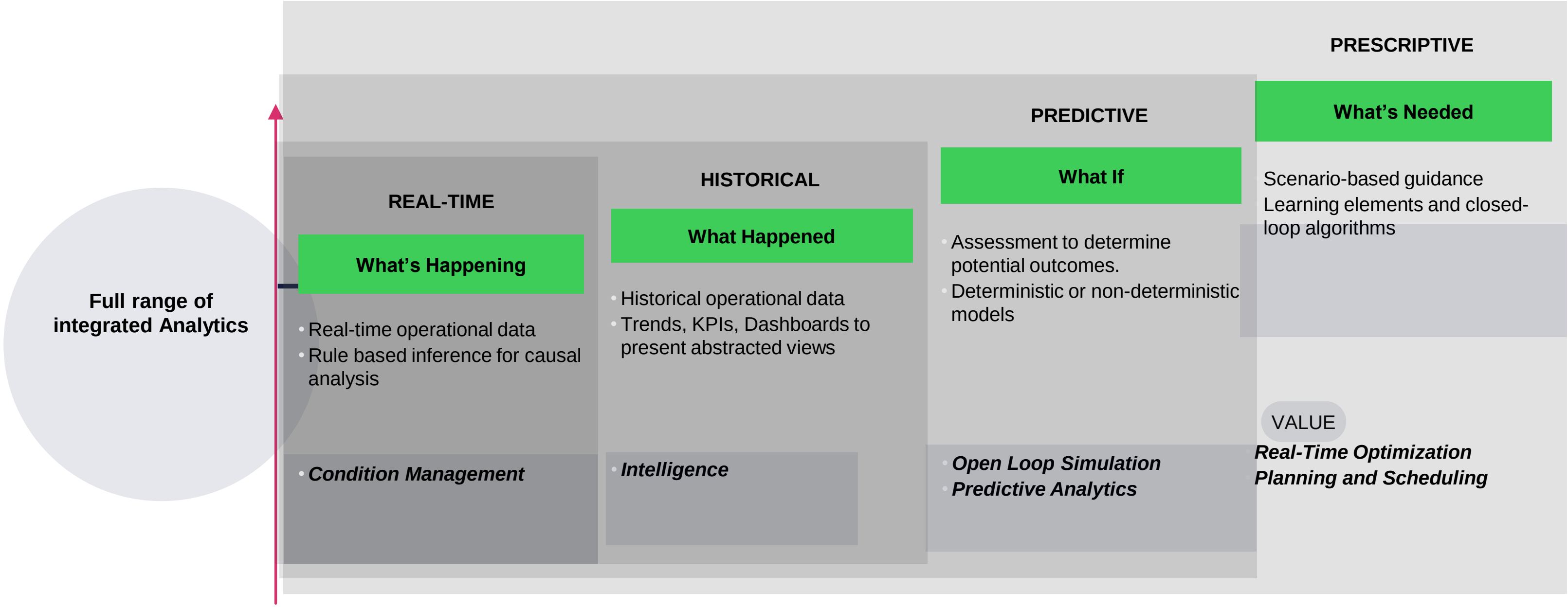
Pervasively for rapid actions



Innovating Information Sharing

Plan for AI automation to augmentation

based on graded probability



Full range of integrated Analytics

REAL-TIME

What's Happening

- Real-time operational data
- Rule based inference for causal analysis
- *Condition Management*

HISTORICAL

What Happened

- Historical operational data
- Trends, KPIs, Dashboards to present abstracted views
- *Intelligence*

PREDICTIVE

What If

- Assessment to determine potential outcomes.
- Deterministic or non-deterministic models
- *Open Loop Simulation*
- *Predictive Analytics*

PRESCRIPTIVE

What's Needed

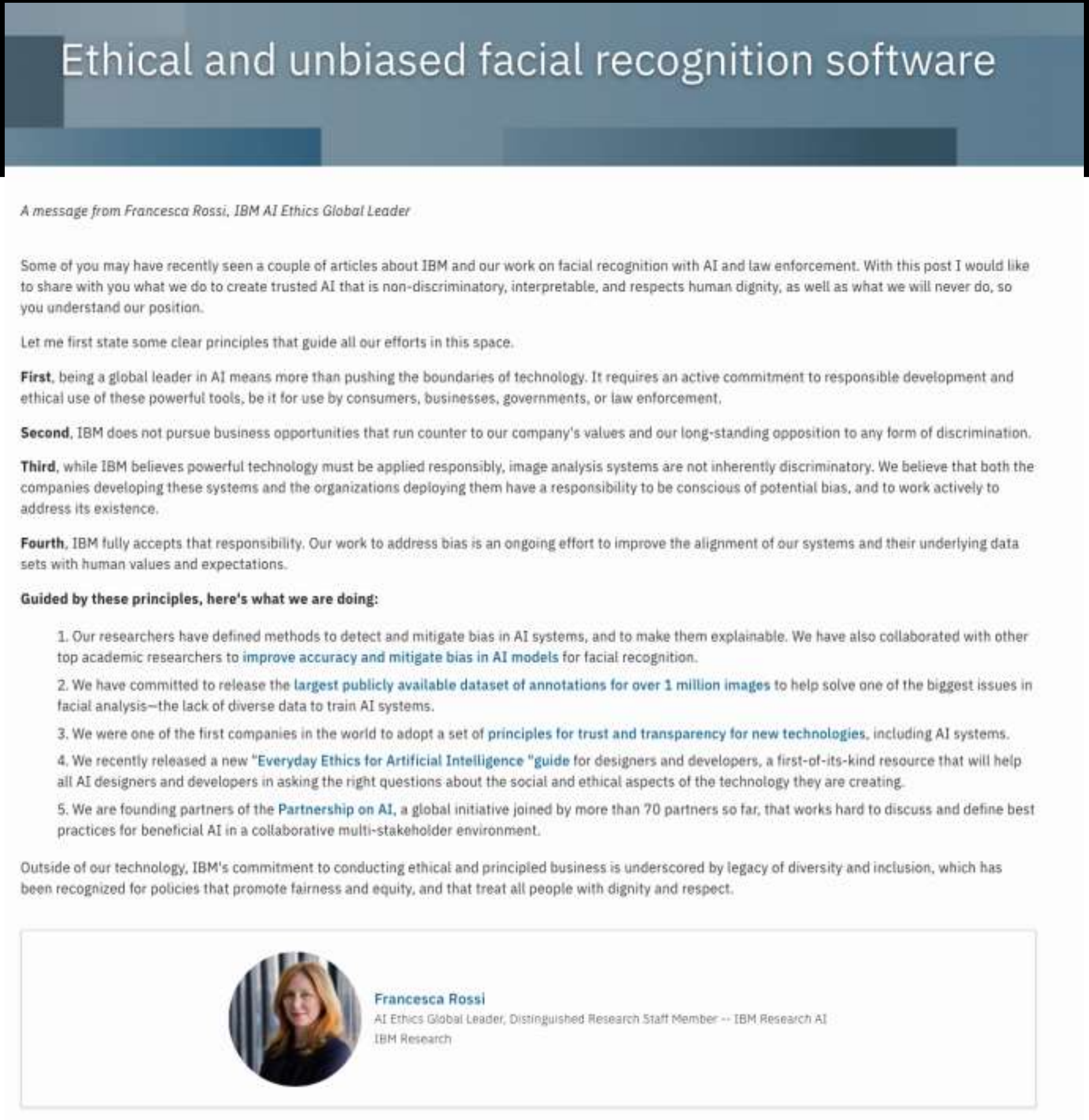
Scenario-based guidance

Learning elements and closed-loop algorithms

VALUE

Real-Time Optimization

Planning and Scheduling



Ethical and unbiased facial recognition software

A message from Francesca Rossi, IBM AI Ethics Global Leader

Some of you may have recently seen a couple of articles about IBM and our work on facial recognition with AI and law enforcement. With this post I would like to share with you what we do to create trusted AI that is non-discriminatory, interpretable, and respects human dignity, as well as what we will never do, so you understand our position.

Let me first state some clear principles that guide all our efforts in this space.

First, being a global leader in AI means more than pushing the boundaries of technology. It requires an active commitment to responsible development and ethical use of these powerful tools, be it for use by consumers, businesses, governments, or law enforcement.

Second, IBM does not pursue business opportunities that run counter to our company's values and our long-standing opposition to any form of discrimination.

Third, while IBM believes powerful technology must be applied responsibly, image analysis systems are not inherently discriminatory. We believe that both the companies developing these systems and the organizations deploying them have a responsibility to be conscious of potential bias, and to work actively to address its existence.

Fourth, IBM fully accepts that responsibility. Our work to address bias is an ongoing effort to improve the alignment of our systems and their underlying data sets with human values and expectations.

Guided by these principles, here's what we are doing:

1. Our researchers have defined methods to detect and mitigate bias in AI systems, and to make them explainable. We have also collaborated with other top academic researchers to improve accuracy and mitigate bias in AI models for facial recognition.
2. We have committed to release the largest publicly available dataset of annotations for over 1 million images to help solve one of the biggest issues in facial analysis—the lack of diverse data to train AI systems.
3. We were one of the first companies in the world to adopt a set of principles for trust and transparency for new technologies, including AI systems.
4. We recently released a new "Everyday Ethics for Artificial Intelligence "guide for designers and developers, a first-of-its-kind resource that will help all AI designers and developers in asking the right questions about the social and ethical aspects of the technology they are creating.
5. We are founding partners of the Partnership on AI, a global initiative joined by more than 70 partners so far, that works hard to discuss and define best practices for beneficial AI in a collaborative multi-stakeholder environment.

Outside of our technology, IBM's commitment to conducting ethical and principled business is underscored by legacy of diversity and inclusion, which has been recognized for policies that promote fairness and equity, and that treat all people with dignity and respect.

Francesca Rossi

AI Ethics Global Leader, Distinguished Research Staff Member -- IBM Research AI

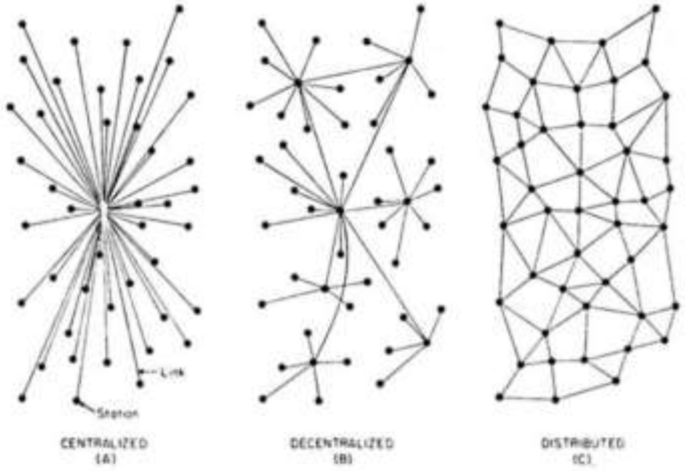
IBM Research

Innovating Information Sharing

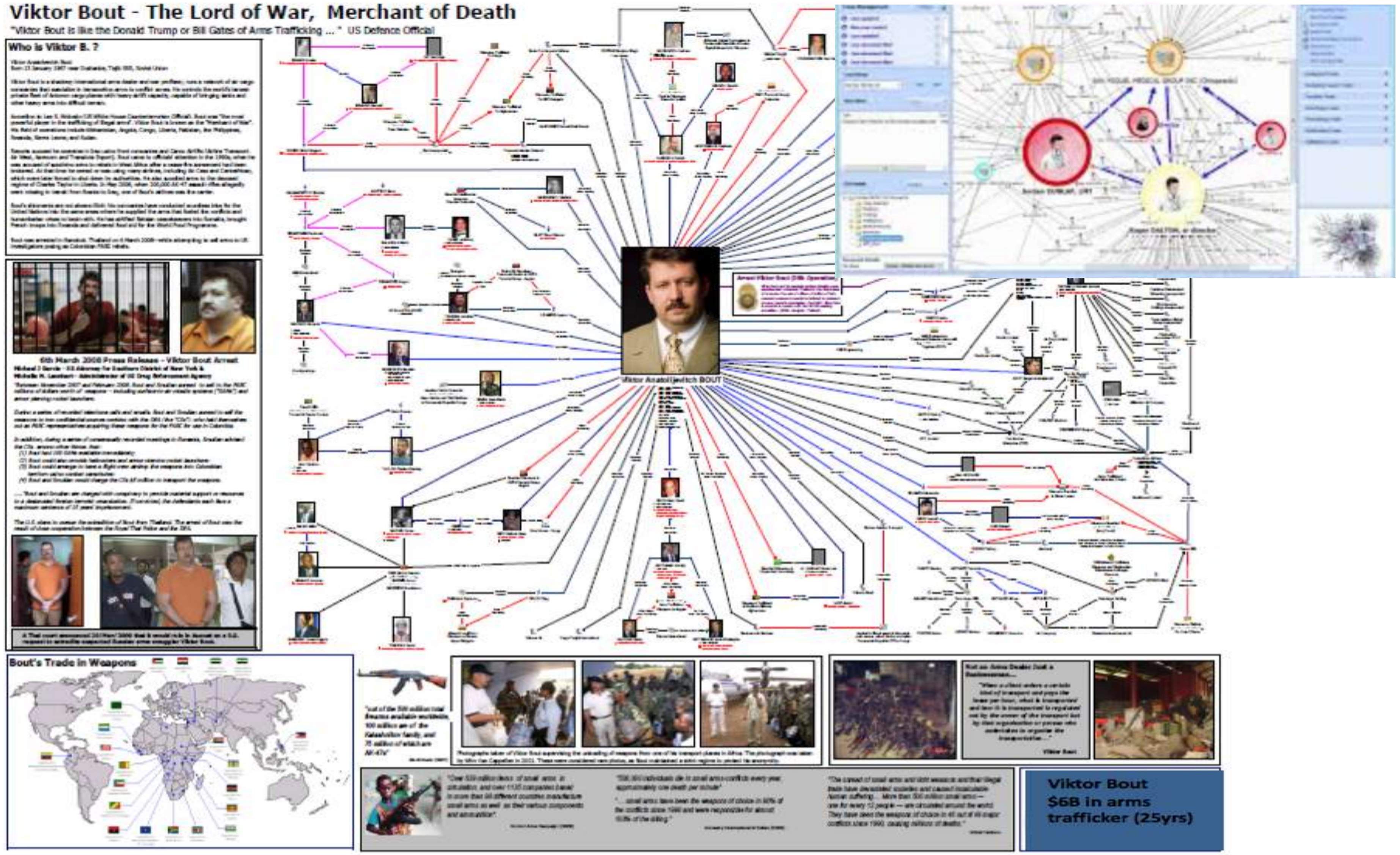
Leverage :

- Blockchain-segmentation for trust building
- Machine learning augmentation using virtual security sensors
- Unbiased aggregation of clear to dark web cyber-tracking

Understanding the blockchain O'REILY



Source: On Distributed Communications Networks, Paul Baran, 1962



Viktor Bout - The Lord of War, Merchant of Death

"Viktor Bout is like the Donald Trump or Bill Gates of Arms Trafficking ... " US Defence Official

Who is Viktor B. ?

6th March 2008 Press Release - Viktor Bout Arrest

Viktor Anatolijevitch BOUT

Bout's Trade in Weapons

Not an Arms Dealer Just a Businessman...

Viktor Bout

Viktor Bout
$6B in arms
trafficker (25yrs)

The Art of the Possible

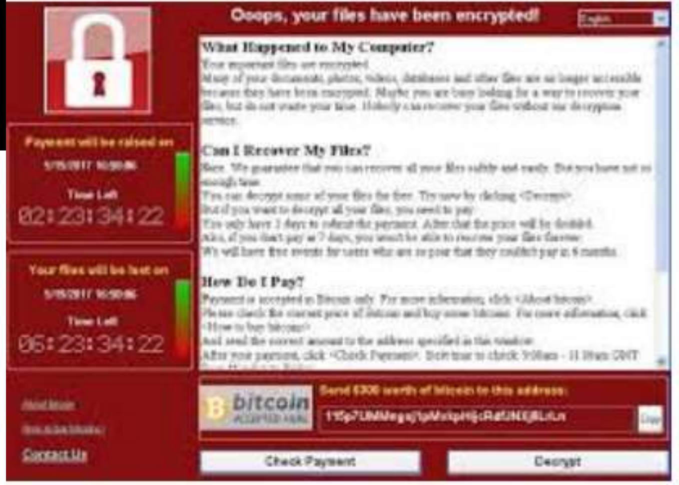
Orchestration

(Beyond Automation…)

Cyber-Security Approach Today – “As is” experience

“Bane & OX cyber-range” exercise debriefing with journalist calling about breach

Journalists speaks to industry analyst confirming cyber-negligence



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

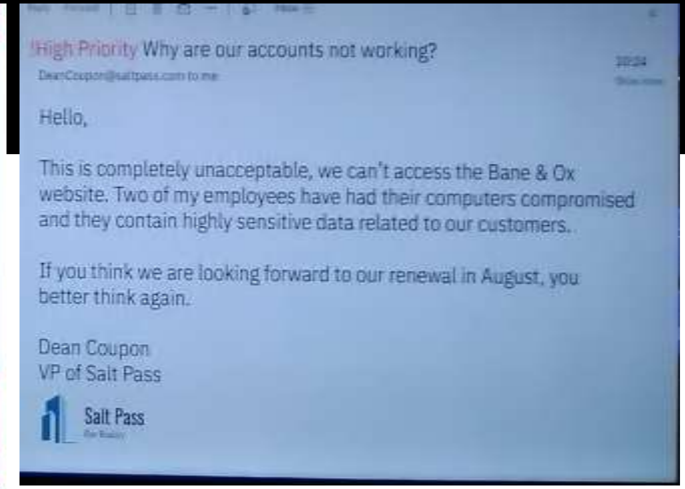
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT

Payment will be raised on
5/15/2017 16:50:06
Time Left
02:23:34:22

Your files will be lost on
5/19/2017 16:50:06
Time Left
06:23:34:22

Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Ransomware demands



High Priority Why are our accounts not working?
DeanCoupon@saltpass.com to me

Hello,

This is completely unacceptable, we can't access the Bane & Ox website. Two of my employees have had their computers compromised and they contain highly sensitive data related to our customers.

If you think we are looking forward to our renewal in August, you better think again.

Dean Coupon
VP of Salt Pass

Partner threatens lawsuits as customers & staff’s PII is exposed

Websites shutdown & start of breach investigation

Nasdaq shutdowns stock & SEC starts investigation

FBI investigates, media publishes, staff is fired, executives testify/go to jail & …

IBM Cyber Resilience

The Art of the Possible – “To Be” cyber-resilient

NOTIFY

Notifications sent

Did you know…

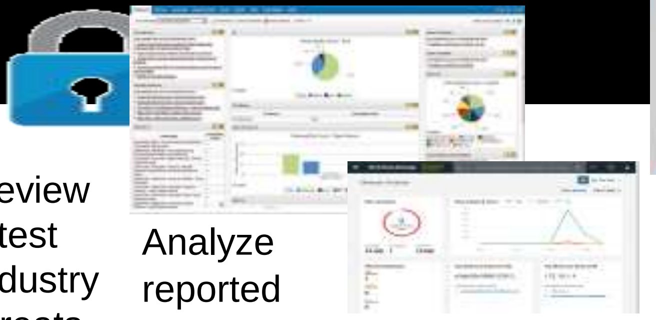
***6 out of 7** hacks are **NOT** detected*

About configuration and/or application/data changes

If not already detected and fixed, client gets inquiry call from journalist about potential breach.

At the same time, operations and security staff receive notifications about configuration and application/data changes to investigate and resolve.

IDENTIFY



Review latest industry threats

Analyze reported problems

Analyze criminal patterns

Start malware analysis / forensics

Manage real threats

Identify impacted systems

Identify breached DBMSes

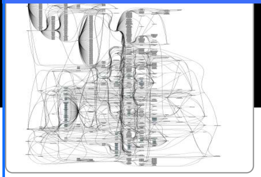
Identify infected apps

Identify criminals networks

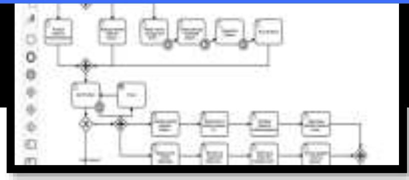
Security staff:
- starts forensics / malware analysis
- researches threats
- reviews security events from helpdesk cyber-security tickets
- analyzes cyber incidents to assess cyber-threats
- reviews the exposure of threats
- identifies cyber networks of criminals / IP addresses
- finds patterns of criminal activities

Networking staff:
- Verifies gaps and depth of penetration

PROTECT / RECOVER



Understand dependencies



Orchestrate Cyber-Incident Recovery

Verify & Deny Access (MFA)

Stop Fraud

Orchestrate Cyber-Protection / Security

Encrypt

Protect Devices

Secure the cloud

IBM BigFix Compliance
Continuous policy enforcement and reporting across endpoints

Report Risk Resolution

Operations Management / Infrastructure staff:
- reviews systems & application dependencies
- recovers in an orchestrated manner from clean copy of malicious configuration & application / data changes.
- produces compliance reports about orchestrated recovery

Networking team:
- Limits access and provides forensic trail

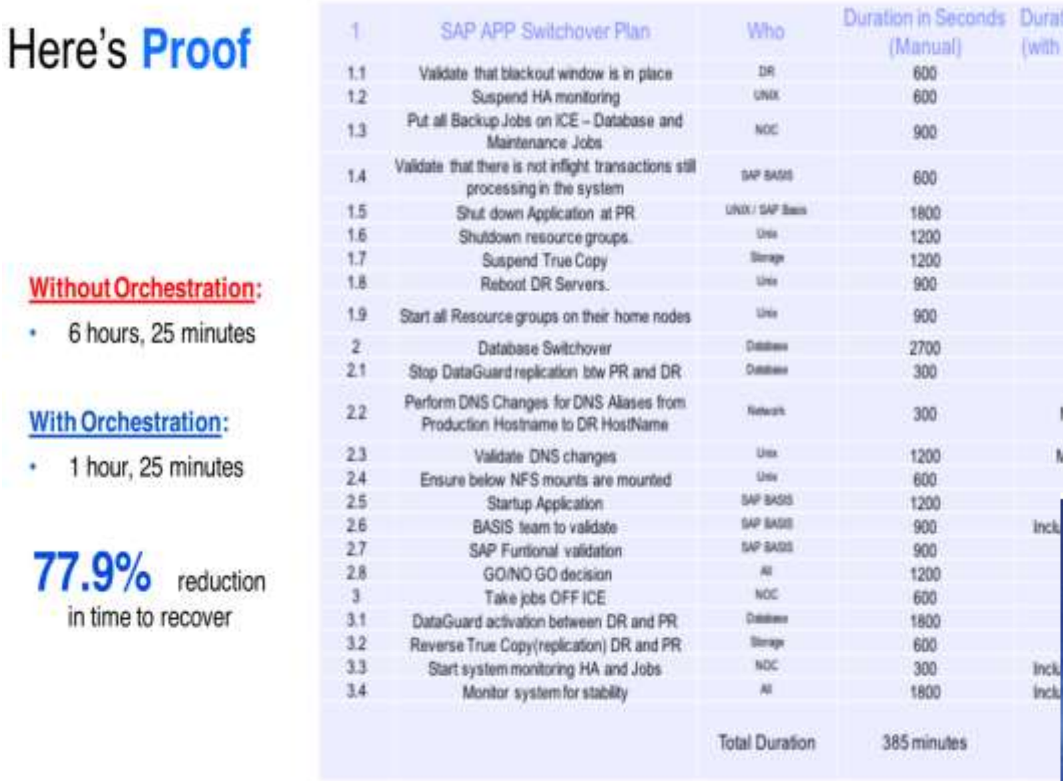
Security staff:
- kicks criminal out & reports on resolution
- reflects the new converted cyber to enterprise risk posture

Outcome: By the time the journalist calls, the cyber-outbreak has been prevented by quickly utilizing with IBM Cyber Resilience

IBM

Innovating Information Sharing

Plan for local & global orchestration



Here's **Proof**

Without Orchestration:

- 6 hours, 25 minutes

With Orchestration:

- 1 hour, 25 minutes

77.9% reduction in time to recover

1	SAP APP Switchover Plan	Who	Duration in Seconds (Manual)	Duration in Seconds (with Orchestration)
1.1	Validate that blackout window is in place	DR	600	60
1.2	Suspend HA monitoring	UNIX	600	360
1.3	Put all Backup Jobs on ICE – Database and Maintenance Jobs	NOC	900	420
1.4	Validate that there is not inflight transactions still processing in the system	SAP BASIS	600	Manual
1.5	Shut down Application at PR	UNIX / SAP Basis	1800	420
1.6	Shutdown resource groups.	Unix	1200	60
1.7	Suspend True Copy	Storage	1200	6
1.8	Reboot DR Servers.	Unix	900	397
1.9	Start all Resource groups on their home nodes	Unix	900	403
2	Database Switchover	Database	2700	120
2.1	Stop DataGuard replication btw PR and DR	Database	300	5
2.2	Perform DNS Changes for DNS Aliases from Production Hostname to DR HostName	Network	300	Manual (300)
2.3	Validate DNS changes	Unix	1200	Manual (1200)
2.4	Ensure below NFS mounts are mounted	Unix	600	60
2.5	Startup Application	SAP BASIS	1200	
2.6	BASIS team to validate	SAP BASIS	900	Incl
2.7	SAP Funtional validation	SAP BASIS	900	
2.8	GO/NO GO decision	All	1200	
3	Take jobs OFF ICE	NOC	600	
3.1	DataGuard activation between DR and PR	Database	1800	
3.2	Reverse True Copy(replication) DR and PR	Storage	600	
3.3	Start system monitoring HA and Jobs	NOC	300	Incl
3.4	Monitor system for stability	All	1800	Incl
		Total Duration	385 minutes	

For IISC presentation, visit:

https://ibm.box.com/v/IISC-2018-09-Presentations

For access, provide your email address to
anyckt@ibm.com

IBM®

Are you ready to become a cyber-diplomat?