



Cybersecurity for Internal Auditors – (Risks) Off The Beaten Track

IIA & WIRC Conference on Internal Audit,
Friday, 6th August, 2021

Assumptions

- You are familiar with cybersecurity and have either been doing CS audit / review
- Or, you are reading and learning about it as you have an audit coming up
- Or, you want to add this to your practice

- In any case, my assumption is that you are familiar with CS jargon and a low level of tech-speak
- I shall try to keep my talk as simple as possible but do feel free to interrupt with a raised hand if needed
- Any form of interaction is welcome

Setting the context



for this
presentation



You Are Audit Professionals


- As members of IIA and ICAI it was anyways a tough job learning the nuances of credit / debit (looks so simple that accounting is just a play of money coming in and going out)
- But then along the way you realize these two words carry conglomerates on their shoulders
- Accounting is a business function which has a role to play across the enterprise
- The profession has moved from pure accounting to becoming trusted advisors

Life was not easy... and...


- Along comes SOX, ITGC, SOC1,2,3 and what have you
- And, what we call Security or Cybersecurity
- Which is also a business function (whether you believe it or not)
- With oversight as well as **interference** in all functions !
- PLUS cybersecurity **MUST** also look at the world outside the business perimeter

Cybersecurity Auditing for the CA

- IT / IS / CS Audit is another onion with layers and layers

- 
- Risk,
 - Asset,
 - Configuration,
 - Change,
 - Patch, Password,
 - Access,
 - Network,
 - Compliance etc

- If this is not complex enough, there is the need to manage compliance with
 - Multiple laws,
 - Regulations / circulars,
 - Standards, and
 - Industry frameworks
- To all this, apply the principles of
 - CIA,
 - PPT,
 - Non-repudiation,
 - least privilege,
 - defense-in-depth,
 - maturity etc ...
 - and now zero trust



**Then above all this is the ‘demon’
of them all: “technology” which
one needs to learn...**

At times one may think (frustratingly) whether it
would have been better to pursue engineering
rather than commerce or economics

This is a Huge Responsibility

A responsibility to bring change. And change is the most difficult thing to bring about, whether within or without

Huge Responsibility - yes

To get your client off the beaten track and to understand that it is *DATA* that is the ultimate asset and not the mean machines they own!

Unfortunately, most organizations focus on *network* security, not *data* security.

63% of organizations deploy new IT prior to having appropriate *data security* measures in place.



A Known Path Well Travelled in Cybersecurity Risk

The (Risk) Path Well Travelled

- The Risks we know and commonly assess (these are find acceptance in most RR)
 - Phishing
 - Insider threat
 - Compliance
 - Ransomware
 - APT
 - DOS
 - Pandemic
 - Natural Disasters
 - Etc...
- Process risks
 - Standard responses,
 - Risk register visited once a year,
 - No risk owner
- Case of a client company: Risk ownership is part of CIO and ERM and residual risk decisions are with CISO

The (Risk) Path Well Travelled

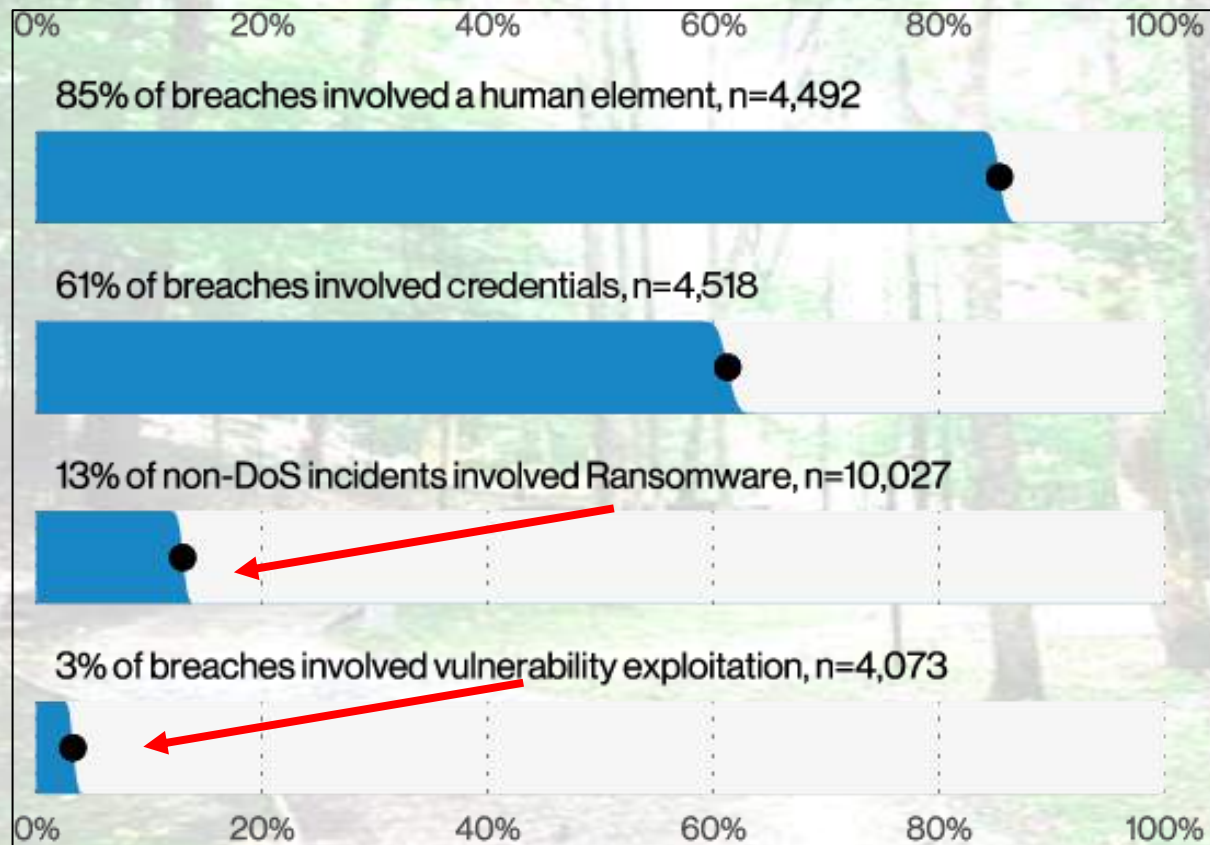


Figure 7. Select action varieties (n=4,073)



Figure 8. Select impacts of incidents

A Known Path Well Travelled in Cybersecurity Risk



Time For Us to Get Off The Beaten (Cybersecurity Risk) Path

Getting Off The Beaten Track

- Look into the future and consider new risks .. They may futuristic but how soon the future will be upon us is anyone's guess
 - Privacy related issues
 - AI based
 - Air gapped infrastructure
- But the off beaten track includes what we are not doing in the present
 - Diligence (for example – Data Classification, Roles / Responsibilities, Awareness)
 - Proactive and preventive action

**Take
inspiration
from**

Take inspiration from



Hype Cycle for Emerging Technologies, 2020



The (Risk) Path Well Travelled

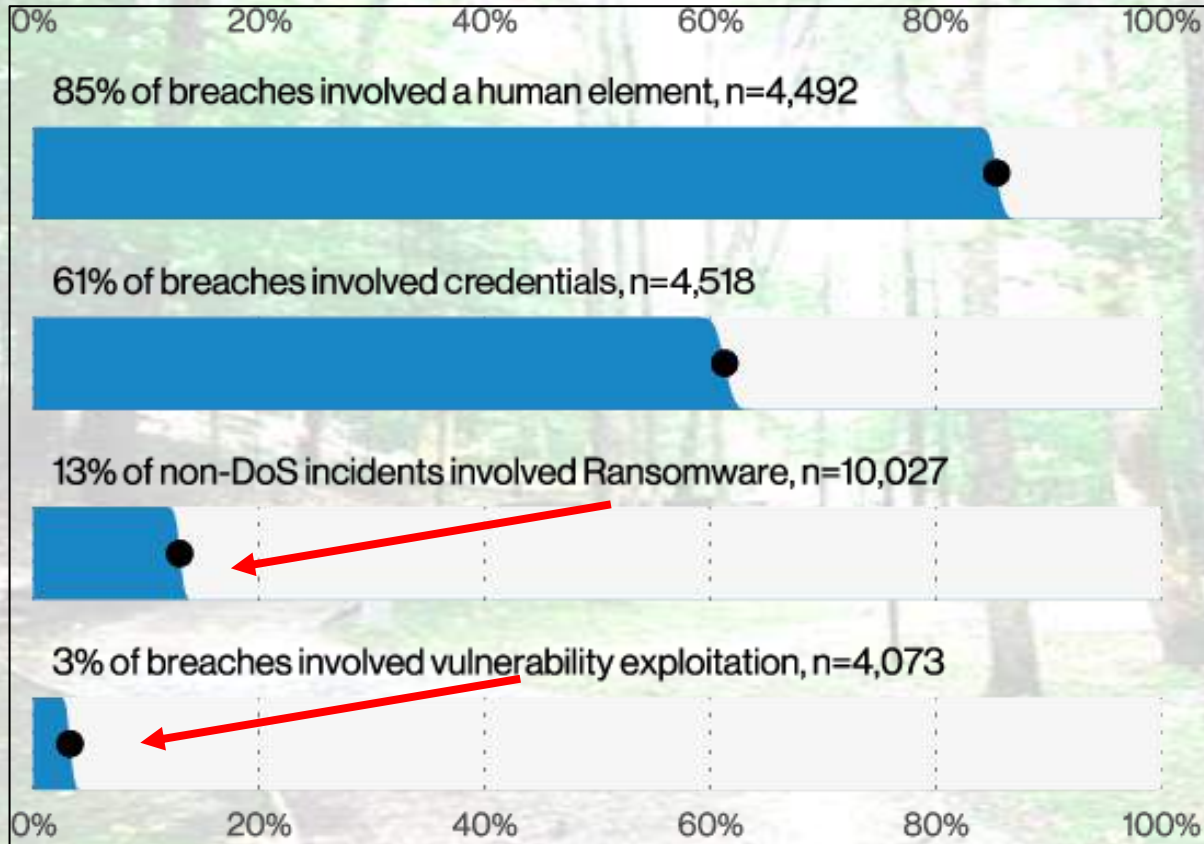


Figure 7. Select action varieties (n=4,073)

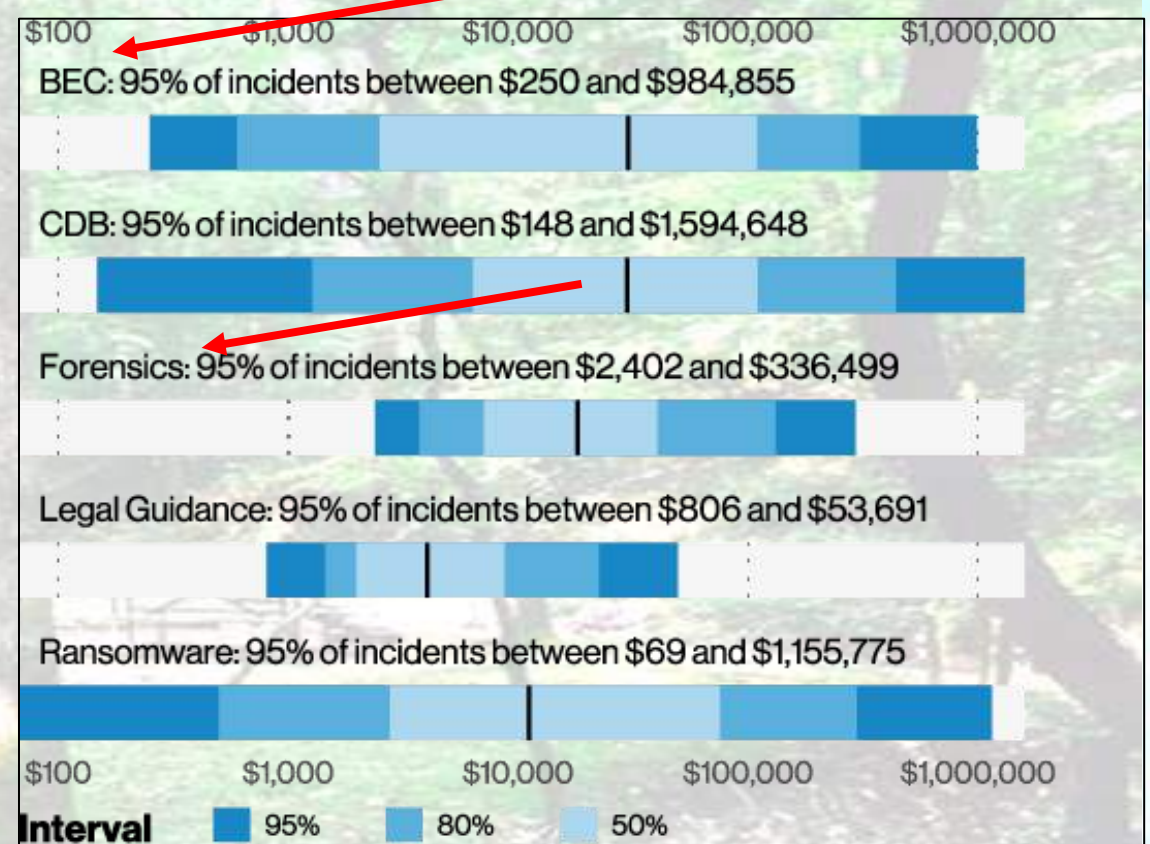


Figure 8. Select impacts of incidents



Save the Axolotl

Dangers of Accelerated Biodiversity Loss

WORLD
ECONOMIC
FORUM

“All businesses should account for ecological risks to their operations and reputations, yet few do: a recent study of Fortune 500 companies found that nearly half mentioned biodiversity in their sustainability reports, but only five set specific, measurable and timebound targets. **Nature-related risks are undervalued in business decision-making.”**

<http://reports.weforum.org/global-risks-report-2020/save-the-axolotl/>

Global Risks 2020: An Unsettled World



“One such area is artificial intelligence (AI). According to the UN’s International Telecommunication Union, it will take “massive interdisciplinary collaboration” to unlock AI’s potential. But because **AI can also bring significant risk, multilateral cooperation is needed to address challenges such as security, verification, “deepfake” videos, mass surveillance and advanced weaponry.”**

<http://reports.weforum.org/global-risks-report-2020/chapter-one-risks-landscape/>

FIGURE 1.1

Short-Term Risk Outlook

Percentage of respondents expecting risks to increase in 2020

Multistakeholders

	Economic confrontations	78.5%	
	Domestic political polarization	78.4%	
	Extreme heat waves	77.1%	
	Destruction of natural ecosystems	76.2%	
	Cyberattacks: infrastructure	76.1%	#5
	Protectionism on trade/investment	76.0%	
	Populist and nativist agendas	75.7%	
	Cyberattacks: theft of money/data	75.0%	#8
	Recession in a major economy	72.8%	
	Uncontrolled fires	70.7%	













FIGURE 1.2

Long-Term Risk Outlook

Top 10 risks by likelihood and impact over the next 10 years

Multistakeholders

Likelihood

-  Extreme weather
-  Climate action failure
-  Natural disaster
-  Biodiversity loss
-  Human-made environmental disasters
-  Data fraud or theft #6
-  Cyberattacks #7
-  Water crises
-  Global governance failure
-  Asset bubble

Impact

-  Climate action failure
-  Weapons of mass destruction
-  Biodiversity loss
-  Extreme weather
-  Water crises
-  Information infrastructure breakdown #6
-  Natural disasters
-  Cyberattacks #8
-  Human-made environmental disasters
-  Infectious diseases

 Economic  Environmental  Geopolitical  Societal  Technological

Getting Off The Beaten Track

- **Look ahead** at new technologies, policy discussions, geopolitics, online media: all this is your best input for threat intelligence
- **Question all:** audit reports / findings (dive in to the how, when, where and why of the technology, the solution, the control, the justification and operation)
- **Keep the theory of security at the back of your mind** – business is paramount and every solution has to think about them first
- Your lack of understanding of technology (or jargon) is not a sign of weakness but demonstrates your willingness to learn (which is sadly missing in many)

Risks Awaiting Diligent Mitigation

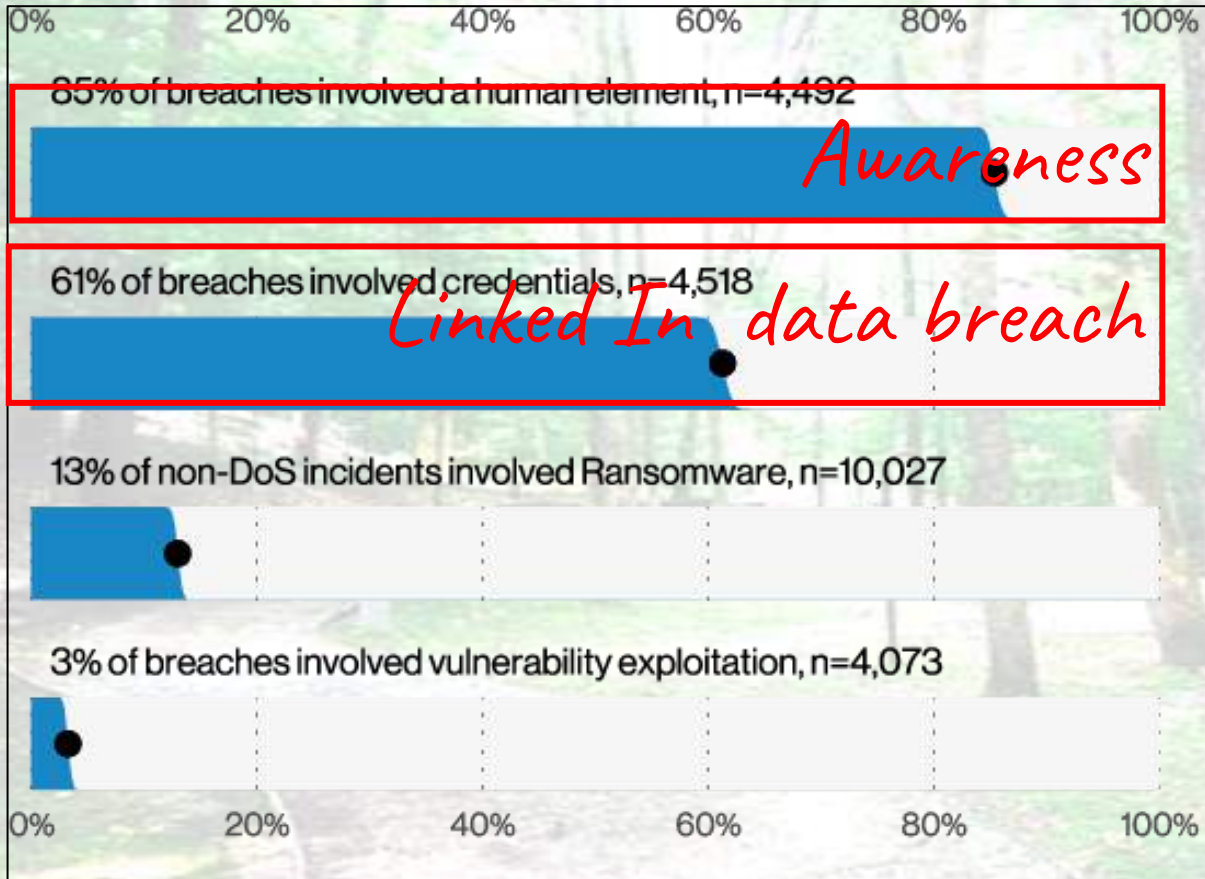


Figure 7. Select action varieties (n=4,073)

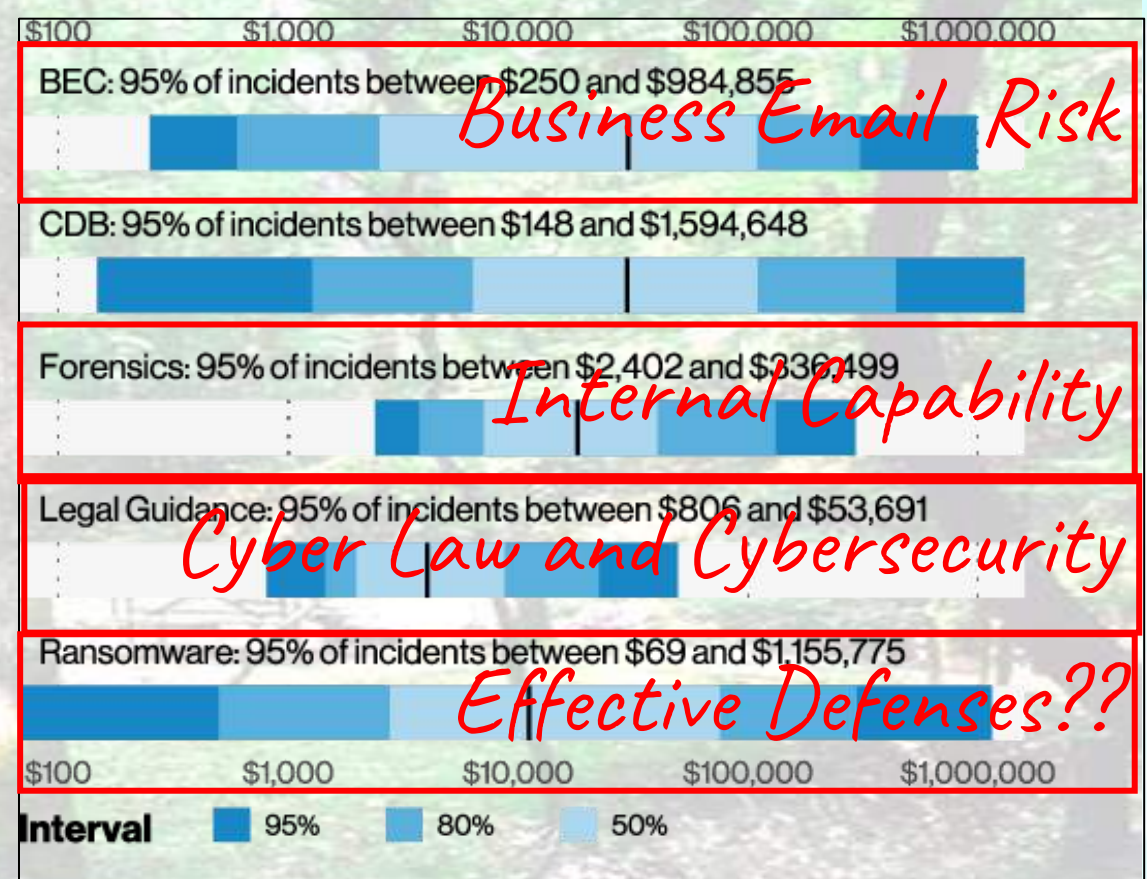


Figure 8. Select impacts of incidents

Awareness

Linked In data breach

Business Email Risk

Internal Capability

Cyber Law and Cybersecurity

Effective Defenses??



Cybersecurity Risks

Talking Privacy

- PDPB - It is coming - the writing is on the wall.
 - What are a majority of security leaders doing: attending trainings in PDPB
 - It is not even a law
 - We do not know how much it will change
 - These same persons will carry these dubious certifications into new jobs as DPOs
 - Consider the risk and advise (early stage) preparation, or design, or changes in the company
 - This is a huge change and involves change in people, process and technology
- Data governance, architecture, and operations
 - For example - Data classification ... which is not about marking a few documents as confidential
 - And, Identification of PII, SPDI, non personal data
 - And, Awareness among the employees
 - And, Automation of controls because it will be impossible to provide assurance
 - Talking and training PDPB – but no data classification
 - GDPR was not applicable but fundamentals can be extracted

Risks in Thinking

- We are compliant with X Y Z ...
- No encryption in place
- USB is not allowed (in small type - except for a few managers and top management)
- We are compliant with X Y Z ...

Cybersecurity Off The Beaten Track

- **Technology Resources** .. Automation is key but we bring in the “best” cutting edge solution.

BOYZ TOYZ

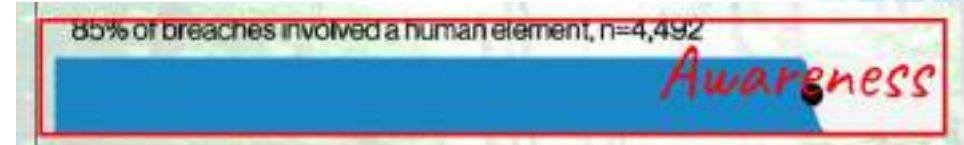
- Disparate systems which may not talk to one another and make life more complex
- Or we avoid it as it is expensive but there is the world of open source which is also not explored.
- Evaluate the effectiveness of utilization (or RoU) with effort and output (DLP, SIEM etc)

Cybersecurity Off The Beaten Track

- **Human Resources ..** The human is more important than the technology which runs the business... what If the server administrator is out of action... or goes rogue
- Analyze attrition and resource utilization among security team
- Is the size of the IS team optimal
- Why only engineers are hired, why not non engineers, and will this stem attrition
- Do you have a growth plan to insource testing
- Awareness ...

Risks Off The Beaten Track

- Once a year sessions is not enough
- Refreshers and new risks
- Training in secure development, testing
- Review the awareness program design and effectiveness
- Obtain user feedback
- Videos on demand sound good, but...
- Correlate results of phishing / vishing drills with trainings
- Look at drill results / effectiveness over past year or quarters
- De-couple security awareness from HR / Training Dept



The human may be the biggest insider risk, but is also the first line of defense – the more knowledge / intelligence the stronger is the human defense

Risks Off The Beaten Track

61% of breaches involved credentials, n=4,518

Linked In data breach

- It happened elsewhere but the risk is to us
- Credentials have been compromised and it is easy to slice and dice data from other dumps (Yahoo, Linked In, Aadhaar, etc)
- Common passwords is a common habit
- No one looks at this risk in the enterprise – it is one which can open up the network
- **Example – Ashley Madison website hacked**

Fifteen thousand government workers - including White House staff - among 37 million identified in Ashley Madison adultery site hack

- Millions of users of the site were identified in the huge global hack
- A 9.7 gigabyte data breach was discovered on Wednesday
- It includes private details as well as sex lives
- Washington D.C. has 15,000 users, 15,000 are from government
- They include the White House and the Senate



BUSINESS

Markets Tech Media Success Video

"No justification." That's how one attorney at the Department of Justice describes his use of cheating site Ashley Madison while in the office.

"That time of my life was just not good personally," he told CNNMoney. And now that he's been exposed? "You look like a moron," he said.

The [massive data breach at Ashley Madison](#) has outed some 32 million users, including some 15,000 email addresses from government and military accounts, indicated by .gov and .mil domains.

Some government officials, like the DOJ attorney, did a better job of covering their tracks: They used personal email addresses like Gmail. At least one used a prepaid credit card for multiple transactions.

<https://money.cnn.com/2015/08/22/technology/ashley-madison-hack-government-workers/index.html>



ETPrime
Personal data of Bharatmatrim

tober 2020

Air India data breach exposes personal information of 4.5 million people

May 2021

The Juspay Data Breach

It was found that sensitive information from over credit and debit card users has been leaked on the

January 2021

Dominos' Customer Data Hacked

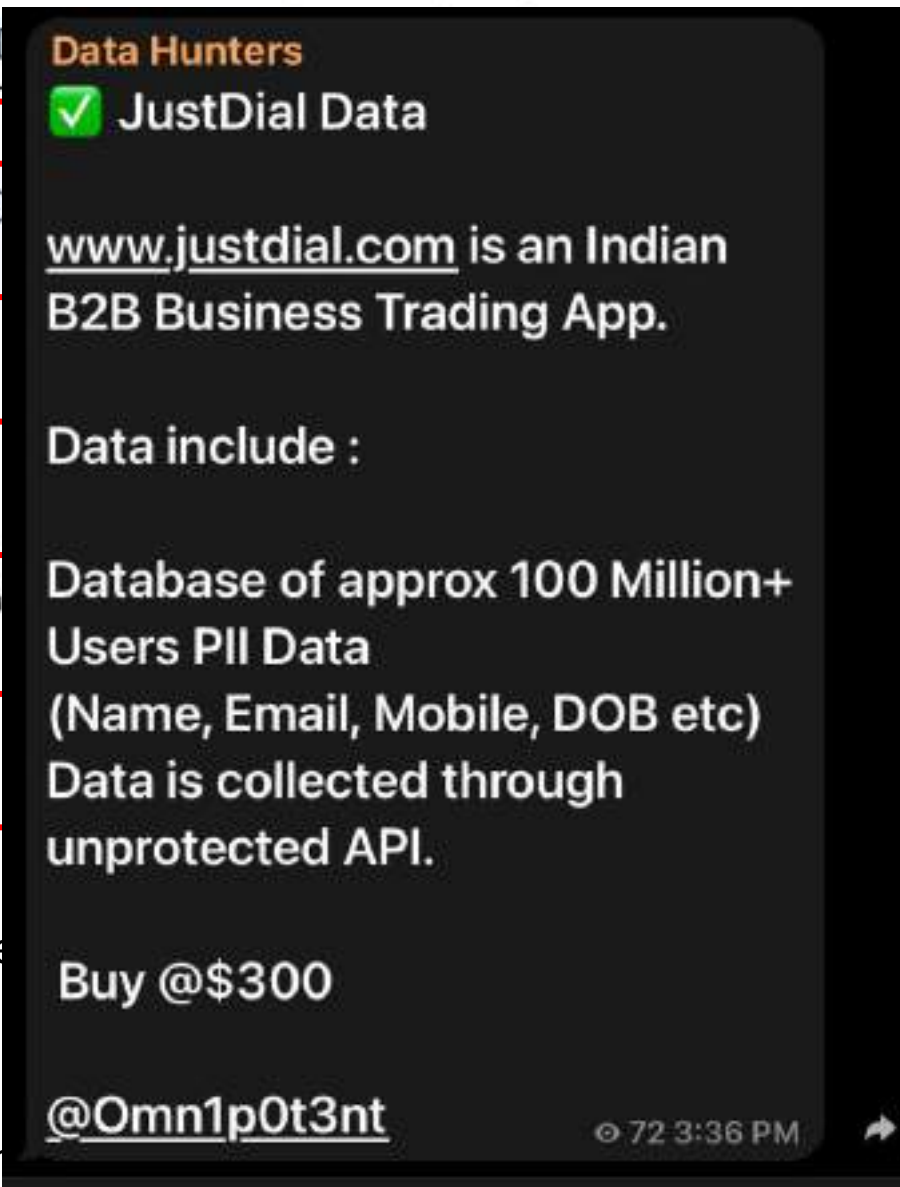
May 2021

Mobikwik Impact: 110 million user de

customer KYC data

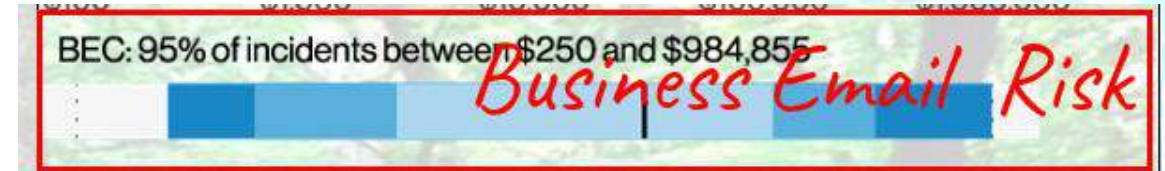
<https://proprivacy.com/privacy-news/air-lr>

<https://timesnext.com/juspay-data-breach-another-feather-on-the-hackers-hat>



Cybersecurity Off The Beaten Track

- BUSINESS EMAIL COMPROMISE (BEC)
- FBI:
 - 2018: \$ 1.29B losses
 - 2019: \$ 1.7B (nearly half of cybercrime losses)
 - 2020: \$ 1.86B losses (number of complaints down to 19,369)
- Risk is not addressed
- Review controls
- Include manual follow up, separate machine / setup



The IC3 saw complaints increase nearly 70% between 2019 and 2020. The top three crimes reported by victims in 2020 were **phishing scams, non-payment/non delivery scams, and extortion**. Officials say victims lost the most money to business email compromise (BEC) scams, romance and confidence schemes, and investment fraud.

[FBI's IC3 Logs 1M Complaints in 14 Months](#)

HOW TO MITIGATE BEC ATTACKS

The following list includes precautionary measures and mitigation strategies for BEC threats:

- Frequently monitor your Email Exchange server for changes in configuration and custom rules for specific accounts
- Consider adding an email banner stating when an email comes from outside your organization so they are easily noticed
- Conduct End User education and training on the BEC threat and how to identify a spear phishing email
- Ensure company policies provide for verification of any changes to existing invoices, bank deposit information, and contact information
- Contact requestors by phone before complying with e-mail requests for payments or personnel records
- Consider requiring two parties sign off on payment transfers

Cybersecurity Off The Beaten Track

Internal capability:

- FORENSICS
- INCIDENT RESPONSE
- CYBER LAW
- LEGAL TEAM & CYBESECURITY

Internal familiarity

- LOCAL LAW ENFORCEMENT
- LOCAL CYBER CELL
- NATIONAL / STATE REPORTING



In Pandemic Times



Cybersecurity Off The Beaten Track

- Work From Home... WFH ... a nice three letter acronym
- Holds a lot of promise and has changed the way we work
- At the same time the threat surface has increased
- Brought millions of weak end points
- With every problem possible that we have been trying to control in the office perimeter
- Nearly 2 years – we have beaten the IT and IS operational issues
- BUT – no one has made an assessment of the risk
 - Home working environment (workplace, family)
 - Size of home and number of family members
 - “additional” use of machine
 - Security of internet access
 - Mental stress in WFH
 - Cost of incident response
 - Effectiveness and practicality of audit
 - Availability and productivity

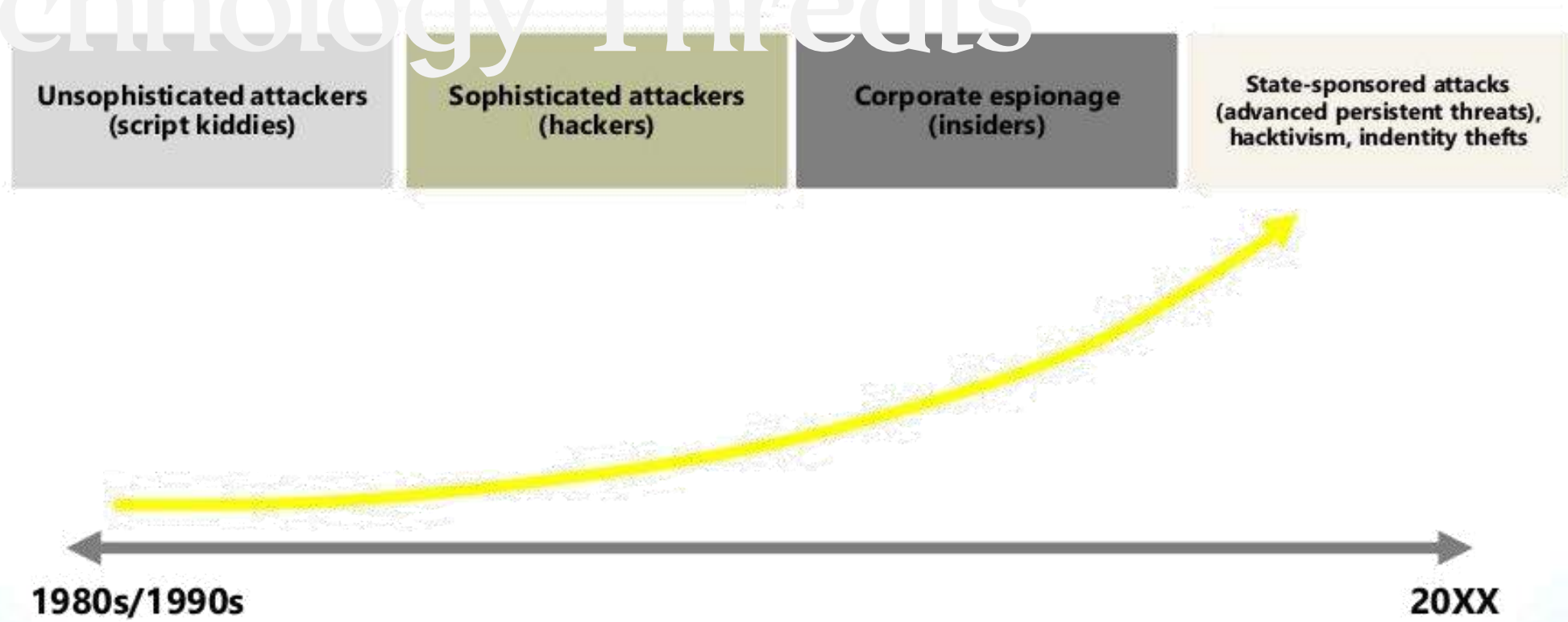
Cybersecurity Off The Beaten Track

- Domain names
 - Who is the administrator
 - What is the associated email address
 - Alerts for payments
 - Risks of like sounding names and cost of acquiring such names
 - Ownership in event of a split in the company
 - Valuation of domain name and inclusion as a brand asset
- Cloud Credentials
 - Name on cloud account
 - Owner of the account access password
 - Backup policy
 - Access controls
 - Reviews

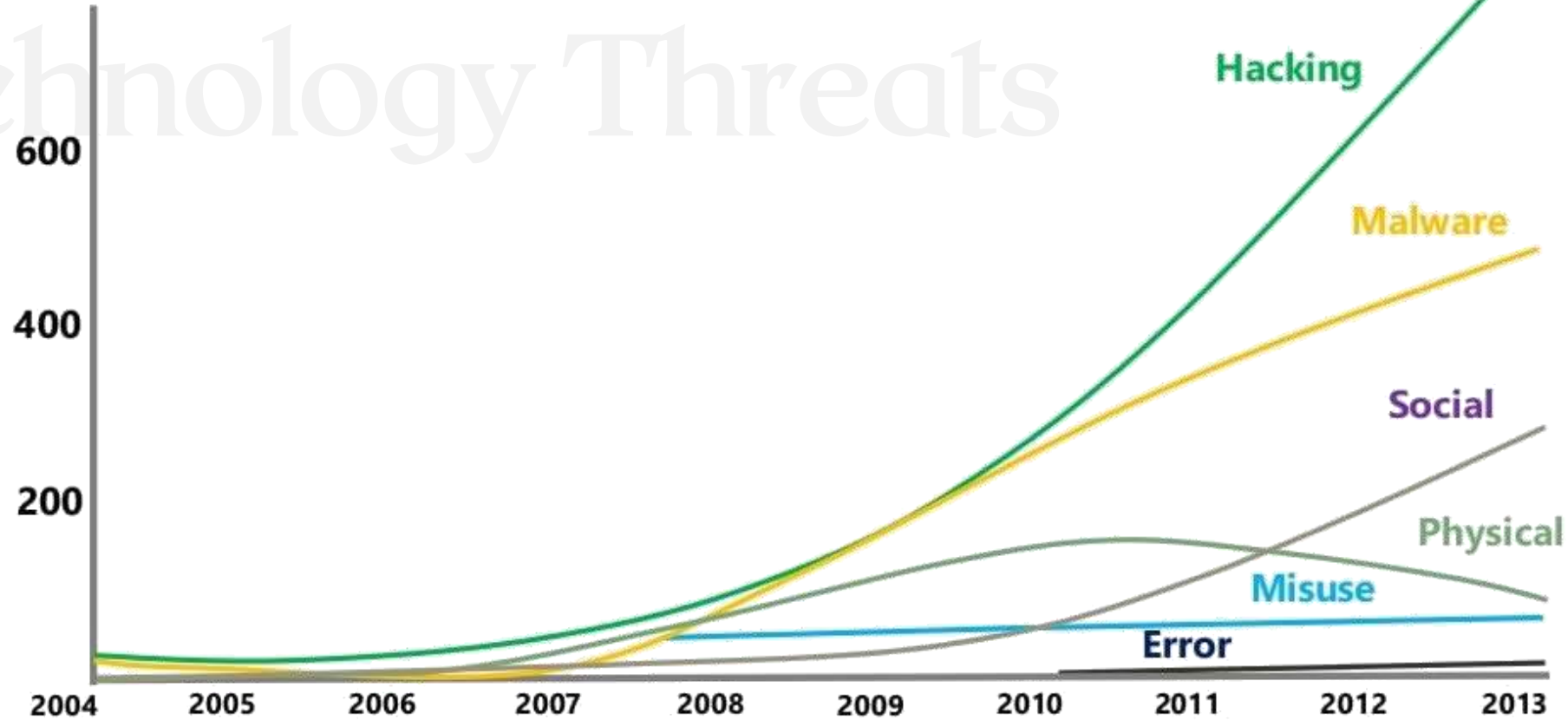
Evolution of Technology & Technology Threats



Evolution of Technology & Technology Threats

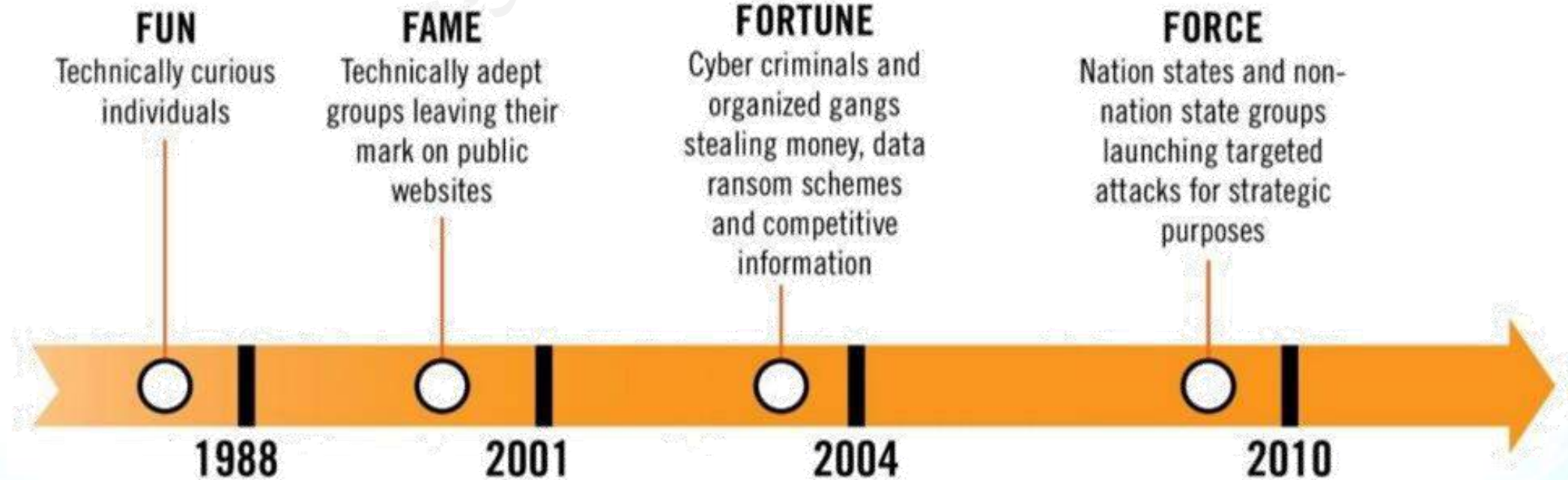


Evolution of Technology & Technology Threats



Source: 2014 Verizon Data Breach Investigations Report

Evolution of Technology & Technology Threats



Look Ahead & Make Your Move(s)

Individually Or As A Business

- Passwordless Authentication
- Cloud Computing
- Cloud Security
- Zero Trust
- Identity and Access Management
- Messaging security
- Network security perimeter
- Endpoint security,
- Secured automation
- Security for trusted third parties.
- Mobile device security
- Protecting digital data
- Rise of Automotive Hacking
- Supply Chain

The Future Is (Actually) Not
Known To ANYONE... Human
Beings Can Only Indulge In
Predictive Speculation

Big Risks / Threats To Look Out For In The Short Term

Supply Chain

Solarwinds, Kaseya

Cloud

AWS, Azure

Global Outages

Akamai, Fastly

Network Fragility

Cyberwar, Critical Infra, Wannacry

Digital Life Threats & Risks

Cybercrime, Espionage, Ransomware

Missing Regulatory Umbrella

Privacy, Data Protection

The 2020 spike in malicious cyber activity continues into 2021 and is growing

Systemic / design weaknesses are being exploited

Lucrative criminal activities are now mainstream technology issues

No distinction between individuals or entities for attacks by state / non-state actors

Risk cannot be seen as an output of a list of threats and one has to change thinking

Bottom Line

Thank
You