CYBER SECURITY FOR MEDICAL COLLEGES

PRESENTER: BENJAMIN MOSSÉ

THURSDAY, AUGUST 3, 2017

MOSSÉ SECURITY

MOSSÉ SECURITY
THREAT MATTERS

About Me

BENJAMIN MOSSÉ
CEO

- ❖ Chief Executive Officer of Mossé Security
- ❖ Founder of Mossé Cyber Security Institute
- ❖ +10 years of experience in cyber security
- ❖ Graduate of Deakin University - Bachelors in IT Security
- ❖ Presented at over 60 of the top conferences in Australia including AISA, OWASP, Auscert, and Ruxcon
- ❖ Technical data:
  - Delivered over 300 penetration tests
  - Manually compromised over 2000 machines
  - Responded to +100 cyber incidents and breaches

AGENDA

01 CYBER SECURITY 2010 VS. 2017

02 BUILDING A MODERN CYBER SECURITY PROGRAMME

03 15 CYBER SECURITY LEADERSHIP QUESTIONS

04 CONCLUSION & NEXT STEPS

CYBER SECURITY 2010 VS. 2017

MOSSÉ SECURITY
THREAT MATTERS

2010 CYBER SECURITY: PROTECT THE CASTLE

- **Metaphor:** “Build an impenetrable castle”
- **Strategy:** Defence-in-Depth (multiple layers of security)
- **Threat Model:**
  - Network vulnerabilities and exploitation
  - Application vulnerabilities and exploitation
- **Security Investments:**
  - Network firewall(s)
  - Two-factor authentication
  - Application security
  - Vulnerability scanning and patch management
  - Password policies

2010 TOP CONCERNS

- Website Defacement
- SQL Injection
- iFrame Injection
- Cross-Site Scripting
- Weak Passwords
- Adware, Spyware, Trojans, Worms, Botnets
- Spam Emails
- Denial of Service Attacks
- Outdated SSL Certificates

WHAT HAS CHANGED SINCE 2010

- BYOD (unmanaged laptops and mobile phones, multiple OS)
- Third party outsourcing (the cloud)
  - Software-as-a-Service
  - Infrastructure-as-a-Service
  - Database-as-a-Service

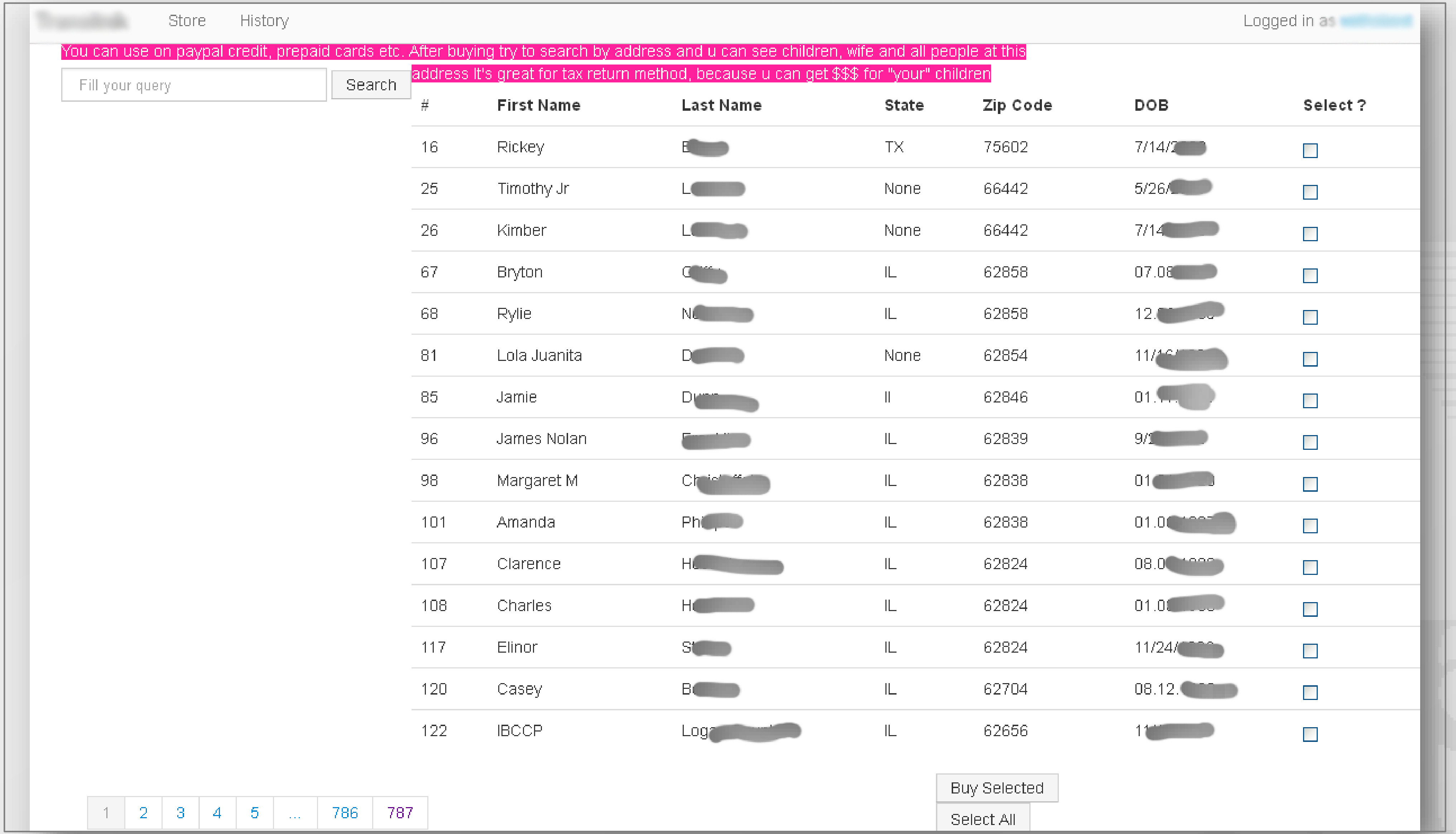
Azure, AWS, Google Cloud offer better infrastructure security than many companies can afford to build on their own

- Windows built-in security features:
  - Anti-virus, anti-ransomware
  - Application whitelisting
  - Endpoint detection and response
  - Exploit mitigations
- Web frameworks built-in protections

WHAT HAS CHANGED SINCE 2010 (Cont.)

- Industrialisation of computer hacking:
  - Cost of attack tools has decreased
  - Availability of free hacking resources has increased
  - A mature underground market for cyber criminals has emerged
  - Adversaries are organised, well funded and persistent
- Commercialisation of computer hacking:
  - Ransoms
  - Blackmail
  - Fraud
  - Sabotage
  - Data Theft
  - Espionage

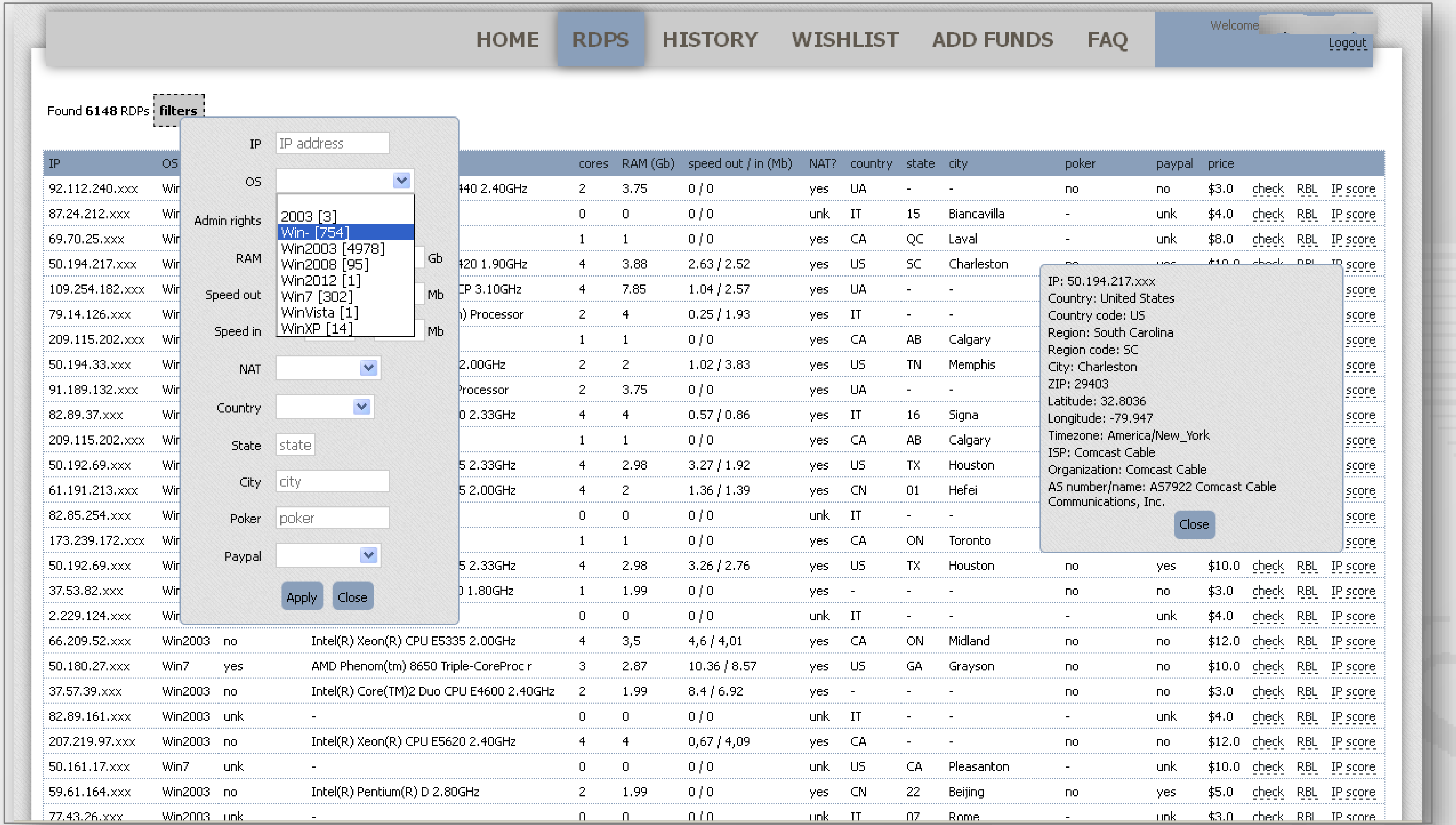
UNDERGROUND MARKET FOR IDENTITIES



You can use on paypal credit, prepaid cards etc. After buying try to search by address and u can see children, wife and all people at this address It's great for tax return method, because u can get $$$ for "your" children

#	First Name	Last Name	State	Zip Code	DOB	Select ?
16	Rickey	[redacted]	TX	75602	[redacted]	□
25	Timothy Jr	[redacted]	None	66442	[redacted]	□
26	Kimber	[redacted]	None	66442	[redacted]	□
67	Bryton	[redacted]	IL	62858	[redacted]	□
68	Rylie	[redacted]	IL	62858	[redacted]	□
81	Lola Juanita	[redacted]	None	62854	[redacted]	□
85	Jamie	[redacted]	Il	62846	[redacted]	□
96	James Nolan	[redacted]	IL	62839	[redacted]	□
98	Margaret M	[redacted]	IL	62838	[redacted]	□
101	Amanda	[redacted]	IL	62838	[redacted]	□
107	Clarence	[redacted]	IL	62824	[redacted]	□
108	Charles	[redacted]	IL	62824	[redacted]	□
117	Elinor	[redacted]	IL	62824	[redacted]	□
120	Casey	[redacted]	IL	62704	[redacted]	□
122	IBCCP	[redacted]	IL	62656	[redacted]	□

BUYING COMPROMISED MACHINES



Found **6148** RDPs **filters**

IP: IP address

OS:

2003 [3]
Win- [754]
Win2003 [4978]
Win2008 [95]
Win2012 [1]
Win7 [302]
WinVista [1]
WinXP [14]

Admin rights

RAM Gb

Speed out Mb

Speed in Mb

NAT

Country

State: state

City: city

Poker: poker

Paypal

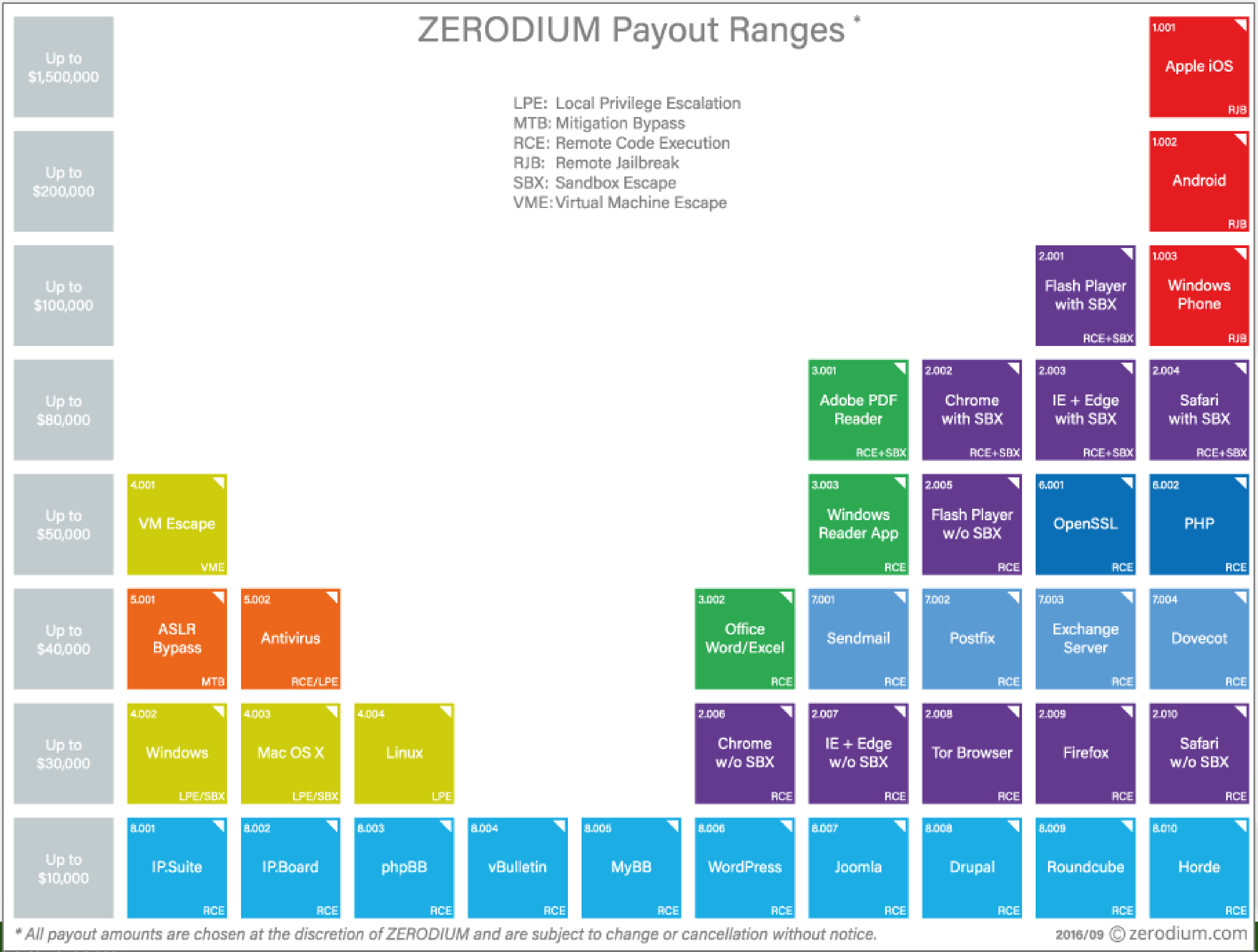
Apply Close

IP	OS			cores	RAM (Gb)	speed out / in (Mb)	NAT?	country	state	city	poker	paypal	price			
92.112.240.xxx	Win		440 2.40GHz	2	3.75	0 / 0	yes	UA	-	-	no	no	$3.0	check	RBL	IP score
87.24.212.xxx	Win			0	0	0 / 0	unk	IT	15	Biancavilla	-	unk	$4.0	check	RBL	IP score
69.70.25.xxx	Win			1	1	0 / 0	yes	CA	QC	Laval	-	unk	$8.0	check	RBL	IP score
50.194.217.xxx	Win		420 1.90GHz	4	3.88	2.63 / 2.52	yes	US	SC	Charleston	no	yes	$10.0	check	RBL	IP score
109.254.182.xxx	Win		CP 3.10GHz	4	7.85	1.04 / 2.57	yes	UA	-	-						score
79.14.126.xxx	Win		) Processor	2	4	0.25 / 1.93	yes	IT	-	-						score
209.115.202.xxx	Win			1	1	0 / 0	yes	CA	AB	Calgary						score
50.194.33.xxx	Win		2.00GHz	2	2	1.02 / 3.83	yes	US	TN	Memphis						score
91.189.132.xxx	Win		Processor	2	3.75	0 / 0	yes	UA	-	-						score
82.89.37.xxx	Win		0 2.33GHz	4	4	0.57 / 0.86	yes	IT	16	Signa						score
209.115.202.xxx	Win			1	1	0 / 0	yes	CA	AB	Calgary						score
50.192.69.xxx	Win		5 2.33GHz	4	2.98	3.27 / 1.92	yes	US	TX	Houston						score
61.191.213.xxx	Win		5 2.00GHz	4	2	1.36 / 1.39	yes	CN	01	Hefei						score
82.85.254.xxx	Win			0	0	0 / 0	unk	IT	-	-						score
173.239.172.xxx	Win			1	1	0 / 0	yes	CA	ON	Toronto						score
50.192.69.xxx	Win		5 2.33GHz	4	2.98	3.26 / 2.76	yes	US	TX	Houston	no	yes	$10.0	check	RBL	IP score
37.53.82.xxx	Win		0 1.80GHz	1	1.99	0 / 0	yes	-	-	-	no	no	$3.0	check	RBL	IP score
2.229.124.xxx	Win			0	0	0 / 0	unk	IT	-	-	-	unk	$4.0	check	RBL	IP score
66.209.52.xxx	Win2003	no	Intel(R) Xeon(R) CPU E5335 2.00GHz	4	3,5	4,6 / 4,01	yes	CA	ON	Midland	no	no	$12.0	check	RBL	IP score
50.180.27.xxx	Win7	yes	AMD Phenom(tm) 8650 Triple-CoreProc r	3	2.87	10.36 / 8.57	yes	US	GA	Grayson	no	no	$10.0	check	RBL	IP score
37.57.39.xxx	Win2003	no	Intel(R) Core(TM)2 Duo CPU E4600 2.40GHz	2	1.99	8.4 / 6.92	yes	-	-	-	no	no	$3.0	check	RBL	IP score
82.89.161.xxx	Win2003	unk	-	0	0	0 / 0	unk	IT	-	-	-	unk	$4.0	check	RBL	IP score
207.219.97.xxx	Win2003	no	Intel(R) Xeon(R) CPU E5620 2.40GHz	4	4	0,67 / 4,09	yes	CA	-	-	no	no	$12.0	check	RBL	IP score
50.161.17.xxx	Win7	unk	-	0	0	0 / 0	unk	US	CA	Pleasanton	-	unk	$10.0	check	RBL	IP score
59.61.164.xxx	Win2003	no	Intel(R) Pentium(R) D 2.80GHz	2	1.99	0 / 0	yes	CN	22	Beijing	no	yes	$5.0	check	RBL	IP score
77.43.26.xxx	Win2003	unk	-	0	0	0 / 0	unk	IT	07	Rome	-	unk	$3.0	check	RBL	IP score

IP: 50.194.217.xxx
Country: United States
Country code: US
Region: South Carolina
Region code: SC
City: Charleston
ZIP: 29403
Latitude: 32.8036
Longitude: -79.947
Timezone: America/New_York
ISP: Comcast Cable
Organization: Comcast Cable
AS number/name: AS7922 Comcast Cable Communications, Inc.

Close

BUYING AND SELLING SOFTWARE VULNERABILITIES



ZERODIUM Payout Ranges *

LPE: Local Privilege Escalation
MTB: Mitigation Bypass
RCE: Remote Code Execution
RJB: Remote Jailbreak
SBX: Sandbox Escape
VME: Virtual Machine Escape

Up to $1,500,000										1.001 Apple iOS RJB
Up to $200,000										1.002 Android RJB
Up to $100,000									2.001 Flash Player with SBX RCE+SBX	1.003 Windows Phone RJB
Up to $80,000							3.001 Adobe PDF Reader RCE+SBX	2.002 Chrome with SBX RCE+SBX	2.003 IE + Edge with SBX RCE+SBX	2.004 Safari with SBX RCE+SBX
Up to $50,000	4.001 VM Escape VME						3.003 Windows Reader App RCE	2.005 Flash Player w/o SBX RCE	6.001 OpenSSL RCE	6.002 PHP RCE
Up to $40,000	5.001 ASLR Bypass MTB	5.002 Antivirus RCE/LPE				3.002 Office Word/Excel RCE	7.001 Sendmail RCE	7.002 Postfix RCE	7.003 Exchange Server RCE	7.004 Dovecot RCE
Up to $30,000	4.002 Windows LPE/SBX	4.003 Mac OS X LPE/SBX	4.004 Linux LPE			2.006 Chrome w/o SBX RCE	2.007 IE + Edge w/o SBX RCE	2.008 Tor Browser RCE	2.009 Firefox RCE	2.010 Safari w/o SBX RCE
Up to $10,000	8.001 IP.Suite RCE	8.002 IP.Board RCE	8.003 phpBB RCE	8.004 vBulletin RCE	8.005 MyBB RCE	8.006 WordPress RCE	8.007 Joomla RCE	8.008 Drupal RCE	8.009 Roundcube RCE	8.010 Horde RCE

** All payout amounts are chosen at the discretion of ZERODIUM and are subject to change or cancellation without notice.*

2016/09 © zerodium.com

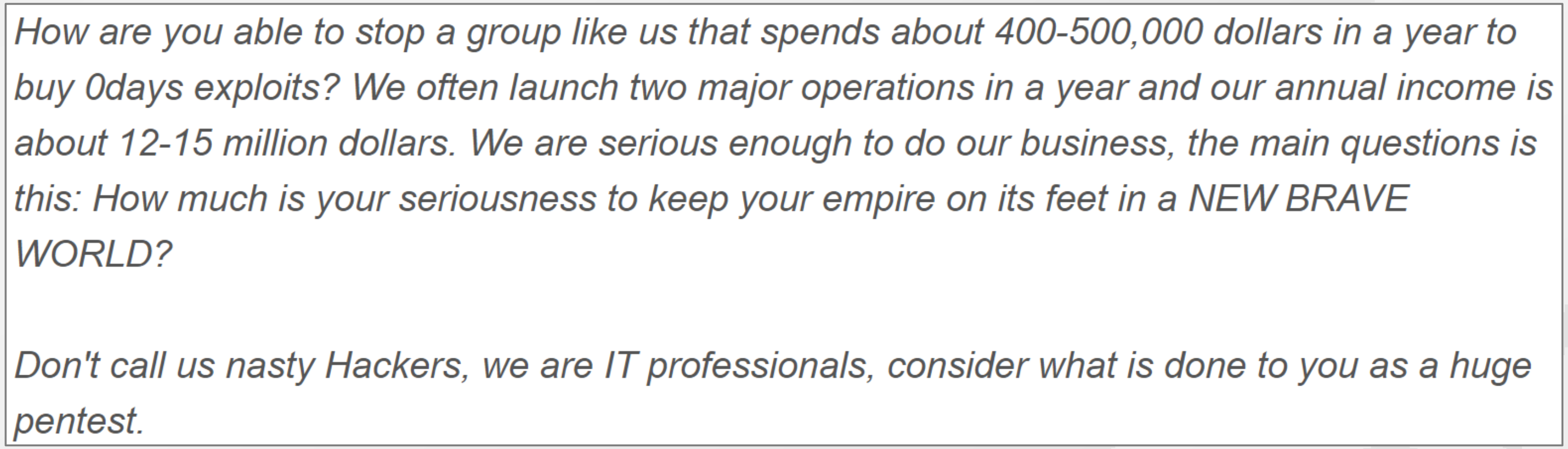
EVERYTHING CAN BE MONETISED

Cyber Crime Statistics	
Credit card number	$1 to $200 per card
Full identity	$15 per identity
Intellectual property	Thousands/Millions
Blackmail	Thousands/Millions
Ransomware	$50 per computer
Twitter	$16 - $325
Vulnerability	$10k – 2M

CYBER CRIME IS A GROWING 1.3 TRILLION DOLLARS INDUSTRY.

ATTACKS AGAINST HBO

- Cyber criminal organisation compromised HBO’s network and stole 1.5 terabytes worth of files:
    - Scripts and videos of unreleased TV shows and movies
    - Company materials (e.g. legal, HR, financials, emails, memos)
    - Personal information of actors (addresses, phone numbers)
- Attackers are asking for a 7.5M ransom to be paid via Bitcoin



How are you able to stop a group like us that spends about 400-500,000 dollars in a year to buy 0days exploits? We often launch two major operations in a year and our annual income is about 12-15 million dollars. We are serious enough to do our business, the main questions is this: How much is your seriousness to keep your empire on its feet in a NEW BRAVE WORLD?

Don't call us nasty Hackers, we are IT professionals, consider what is done to you as a huge pentest.

SCARY MESSAGE

EVEN MODERATELY SKILLED ATTACKERS ARE STILL TOO SOPHISTICATED FOR MOST ORGANISATIONS TO DEFEND AGAINST

INVESTMENTS THAT ARE NO LONGER SUFFICIENT AT PREVENTING ATTACKS

Security Investment	Attacker Response
Secure Coding	Target the developers / sysadmins
Firewall	Target the endpoints
Anti-Virus Software	Obfuscation
Strong Passwords	Steal and re-use NTLM hashes
Intrusion Detection System	Obfuscation
Enterprise Web Proxy	Tunnel through HTTPS/DNS/ICMP
Data Leakage Prevention	Encryption
Data Encryption	Ransomware
Network Segmentation	Compromise network administrators

SCARY MESSAGE

ATTACKERS HAVE FIGURED OUT HOW TO BYPASS ALL TRADITIONAL YOUR SECURITY INVESTMENTS

SECTION SUMMARY

COMPARING THE METAPHORS:

2010

How do I solve weak passwords?

2017 and beyond

How do we deal with blackmail?

QUESTION FOR THE AUDIENCE

WHAT IS YOUR PLAN FOR WHEN CRIMINAL SYNDICATES STEAL ALL OF YOUR MEMBER DATA AND COMPANY MATERIALS, AND BLACKMAIL YOU FOR HUNDREDS OF THOUSANDS OR MILLIONS OF DOLLARS?

BUILDING A MODERN CYBER SECURITY PROGRAMME

MOSSÉ SECURITY
THREAT MATTERS

2017 CYBER SECURITY PROGRAMMES

- **Investment Model:**
  - +/- 40% acquiring the right people, and training them
  - +/- 40% building, maintaining and adhering to security processes
  - +/- 20% acquiring and maintaining critical security technologies
- **Principles:**
  - Culture of IT security
  - Data-driven security
  - Strategy > tactics
  - Incident preparedness
  - Resilience

TRAINING YOUR COMPANY ON INFORMATION SECURITY

Senior Management

- Executive Courses
- Threat Briefings
- Self-Defence
- Cyber Breaches War Games

Employees

- Following Company Processes
- Self-Defence
- Anti-social engineering

IT Personnel

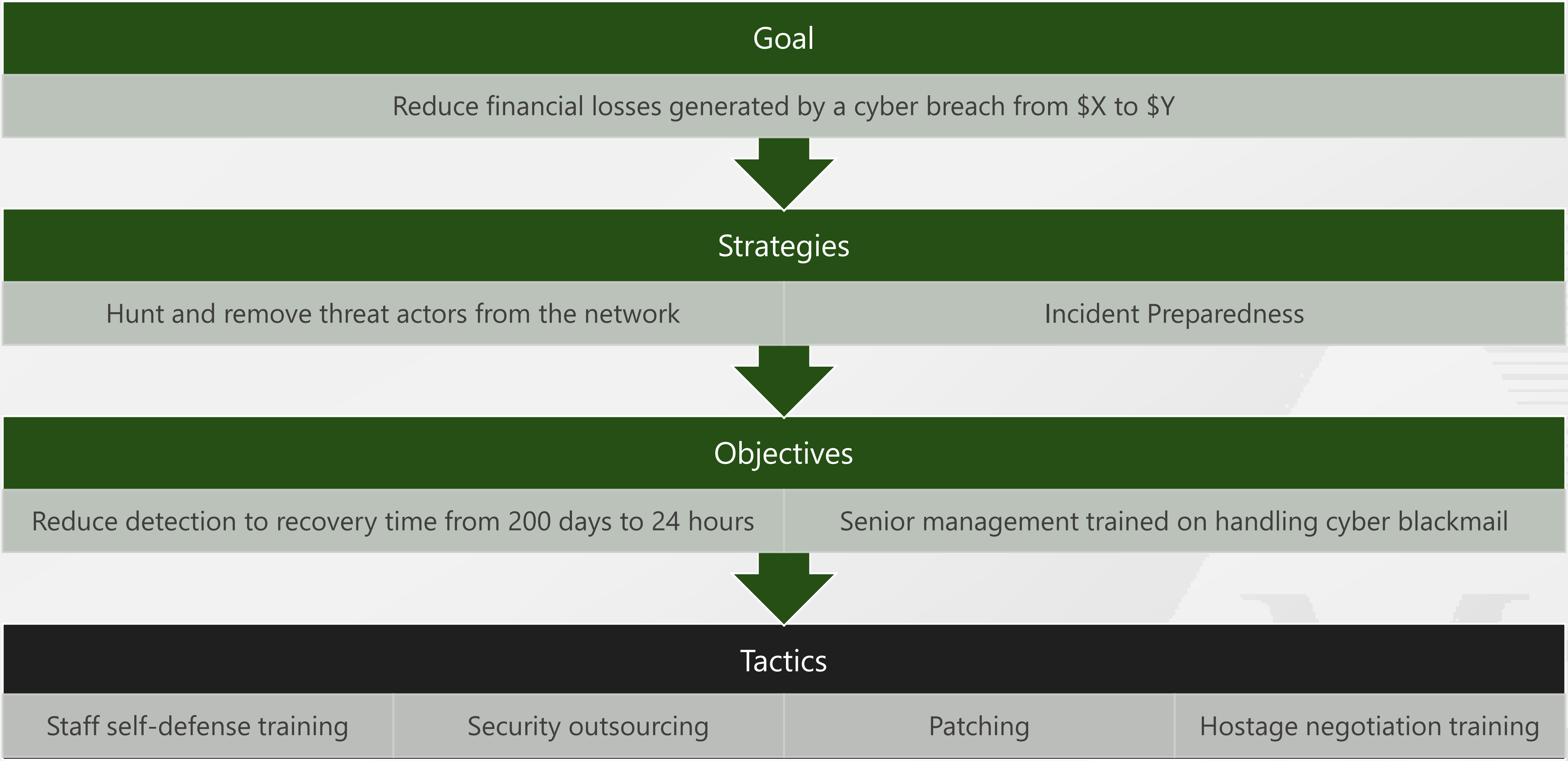
- Network Defence
- Incident Response
- Cyber Breaches War Games

EDUCATION IS WHAT HELPS PEOPLE WORK AS A TEAM

THE MUSICAL CHAIRS OF CYBER BREACHES:

- Board members will consults their lawyer to protect themselves from the exposure
- The Board will point the finger to the CEO
- The CEO will point the finger to the CIO
- The CIO will point the finger to the IT manager
- The IT manager will point the finger to the budget
- The IT engineers will claim ignorance and not having received enough resources
- Ultimately, the customers and the members are the ones loosing out the most

BE MORE STRATEGICAL THAN TACTICAL



Goal

Reduce financial losses generated by a cyber breach from $X to $Y

Strategies

- Hunt and remove threat actors from the network
- Incident Preparedness

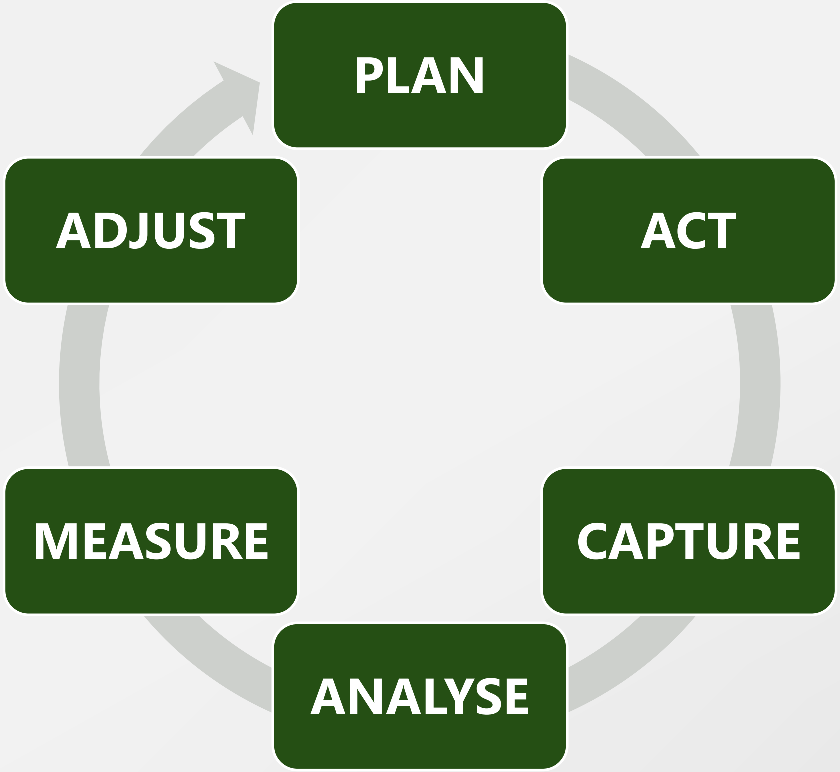
Objectives

- Reduce detection to recovery time from 200 days to 24 hours
- Senior management trained on handling cyber blackmail

Tactics

- Staff self-defense training
- Security outsourcing
- Patching
- Hostage negotiation training

DATA DRIVEN IT-SECURITY



PLAN

ACT

CAPTURE

ANALYSE

MEASURE

ADJUST

EXAMPLES OF MEASURABLE OBJECTIVES
Reduce financial losses generated from cyber breaches from $X to $Y
Reduce the number of intrusions into our network from X to Y over period Z
Reduce average time from detection to recovery from X days to Y hours

INCIDENT PREPAREDNESS

- ❖ What are our top priorities during a security incident?
- ❖ Who are the key people we need to inform?
- ❖ What key questions does our IT department need to be able to inform during an incident?
- ❖ What role must other departments play in responding to the breach? What information do they require to know?
- ❖ When should we inform our clients about the breach?
- ❖ When should we call law enforcement?
- ❖ Who else do we need to notify about the breach? At what point?
- ❖ When do we inform the media? What information do we share with them?
- ❖ **What do we do if we receive no law enforcement support?**

RESILIENCE

- How can you be sure that:
  - You can survive ransomware?
  - You can survive blackmailing?
  - You can survive all your data being deleted?
    - How can we be sure that backups can’t be deleted?
  - You survive sabotage from an internal employee?

These are the big “cyber” questions of today and towards 2025

THE WRONG QUESTIONS WE GET ASKED ALL THE TIME

MOSSÉ SECURITY
THREAT MATTERS

WHAT PRODUCT SHOULD I BUY?????

UPDATE TO WINDOWS 10 PRO RS2+

AND

TURN EVERY SECURITY SETTING ON!

(OR DIE TRYING)

WINDOWS SECURITY FEATURES

Security Controls	Windows Built-In Solutions
Anti-Virus / Anti-Ransomware	Windows Defender
Application Whitelisting	Device Guard, AppLocker
Credentials Protection	Credentials Guard
Endpoint Detection & Response	Advanced Threat Protection
Hard-Drive Encryption	Bitlocker
Exploit Mitigations	EMET, Defender Exploit Guard, ASLR, NX, CFG, HVCI, etc.
Patching	Continuous Security Updates
Passwords Protection	Local Administrator Password Solution (LAPS)

Most of these protections are built-in Windows 10 Pro, at no additional costs

REMAINING SECURITY TECHNOLOGY GAPS

- If you used all the features listed in the previous slides, the remaining security threats you would be facing are:
  - File-less malware (e.g. Word Macros, HTAs, PowerShell, etc.)
  - Social engineering attacks
  - Memory-only attack tools
  - The occasional ransomware, malware, wiper
  - User errors
- Many embedded devices (IoT) have no, or almost no, security. So they'll be the next big problem for us all to address in the next 20 years.

WHAT ABOUT CYBER INSURANCE??!!!

- **What's insured:**
  - Cost investigating and responding to the breach
  - Cost of notifying customers
- **What's not insured:**
  - Damage to reputation / Brand damage
  - Financial losses / Business interruption / Loss of revenue
- **What's not covered:**
  - Anything you untrusted to a third-party vendor if the breach occurred on their systems
  - Unencrypted data, intellectual property, trade secrets
  - Negligence-induced incidents

WHAT ABOUT OUTSOURCING IT SECURITY???!!!

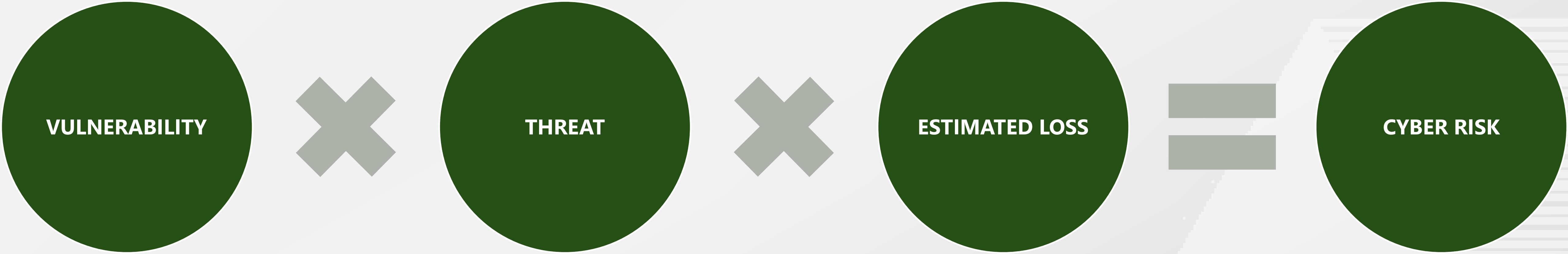
- How are you going to outsource the damages to your reputation?
- How can you be sure that the security vendor(s) you work with are doing their job?
- What gives you confidence that you have the legal firepower to get compensated from a managed security provider if a breach happens on their watch?

Generally speaking, security vendors do not provide any guarantees for the quality of their products and managed services. Neither will they accept any liability or consequences for failing to deliver security that works.

15 CYBER SECURITY LEADERSHIP QUESTIONS

MOSSÉ SECURITY
THREAT MATTERS

CYBER RISKS 101

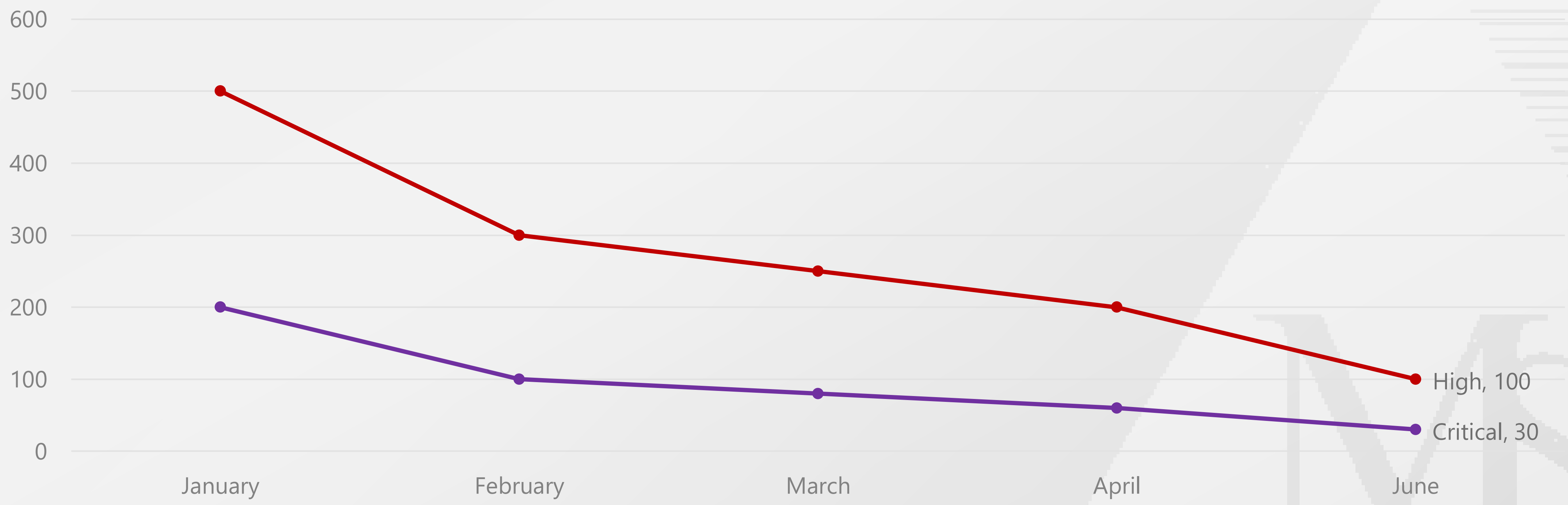


VULNERABILITY × THREAT × ESTIMATED LOSS = CYBER RISK

CYBER RISK is
Your most critical vulnerabilities, exploited by your greatest adversaries, in the worst case scenario possible.

RULE 1: MANAGE YOUR VULNERABILITIES

- How many critical and high risk vulnerabilities do we have today?
- How many vulnerabilities can we mitigate in the next 90 days?
- What resources are required to fix those vulnerabilities? (Calculate in dollars)



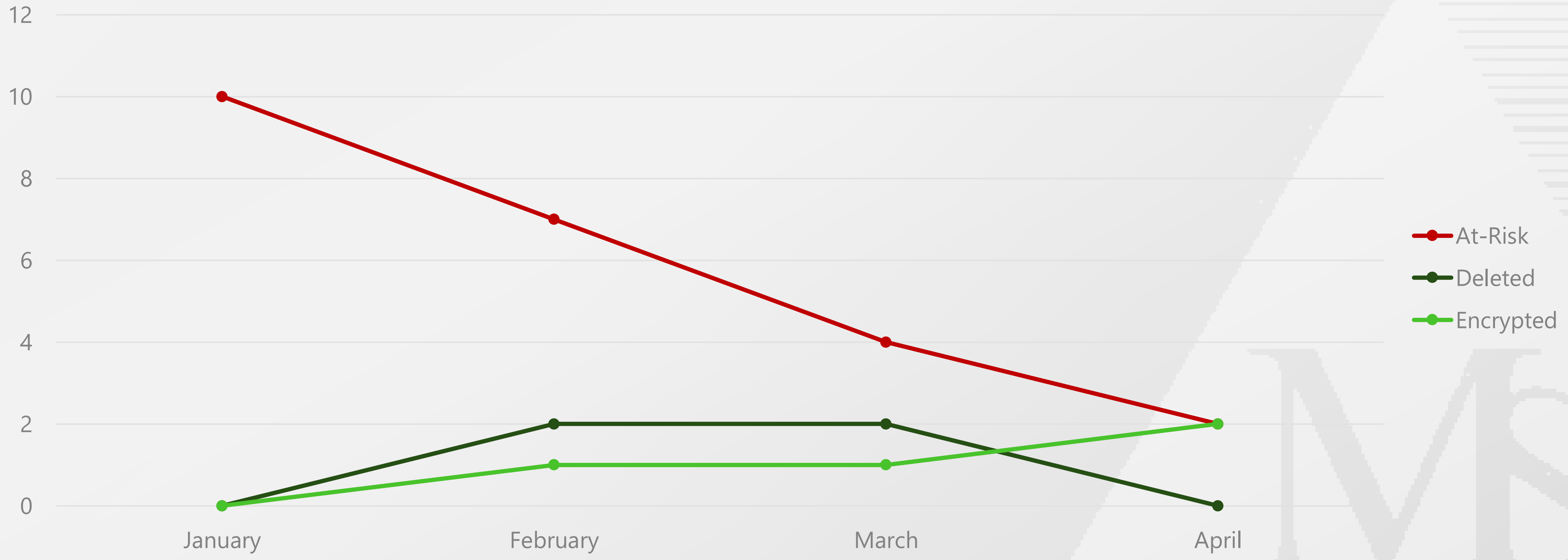
RULE 2: DISRUPT YOUR ENEMIES

- How cyber incidents did we have in the last 90 days?
- For each incident, what risks were we exposed to? (Calculate in dollars)
- How much time did it take us to detect the incidents and recover?
- What resources are required to prevent the attackers from coming back?

Metrics	Current Status	Goals
Number of intrusions	+10	Less than 3
Skill level used to breached in	Basic techniques	Complex techniques
Detection time	227 days	Less than 10 days
Response time	25 days	Less than 48 hours
Impact generated / Value stolen	$250,000.00 AUD and above	Less than $10,000.00 AUD

RULE 3: LIMIT YOUR EXPOSURE

- How much data at risk do we have today?
- How much data can we safely remove in the next 90 days?
- How much data can we safely encrypt and archive in the next 90 days?



RULE 4: MAKING SURE THE PLAN’S SOLID

	Questions
Cost Saving	How are we leveraging our existing investments to solve today’s challenges?
Data Driven	How are we going to measure the effectiveness this round of investment?
Long Term	How are we making sure this round investment will continue to yield results in 12 months?
Feasible	How do we know if we have people with the right knowledge to implement the plan?
Backup Plan	How will we address things if we find we're off track?

GOALS

ACHIEVE THOSE GOALS WITHIN 12 TO 18 MONTHS:

- Train 100% of your staff members on cyber security
- Review your network for active or dormant threat actors
- Remove or encrypt 70% of your data
- Stop and detect the top 200 tactics and techniques employed by attackers (*see the ATT&CK Matrix from MITRE*)
- Prepare an incident response plan and test it twice a year

CONCLUSION

CONCLUSION

- Make a commitment with yourself to become a champion for cyber security in your organisation
- Hold yourself accountable
- Inspire your team members to do the same
- Use the Leadership Questions to monitor your cyber risks and address them quickly

CONTACT US

Mossé Security

Mossé Cyber Security Institute

+61 1300 730 035

contact@mosse-security.com

MOSSÉ SECURITY
THREAT MATTERS