CYBERCRIME & E-FRAUD

Underplaying the Risk to Economic Well Being

ANNESE

A ConvergeOne COMPANY

AGENDA

- Good news!
- Jeopardy
- Central Themes/State of Security
- Cybercrime Unearthed
- What Are Fraudster’s Up To?
- So, Who Protects the Public At-Large
- The Impact is Catastrophic and Pervasive
- Quo Vadimus
- So What, Now What?
- POLICY, PEOPLE, PROCESS, PREVENTION = SUCCESS
- Taking The Political Temperature
- Time for Change is Now

"Good news. Our threats and vulnerability alerts have decreased since we outsourced our network monitoring to China."

LET'S PLAY JEOPARDY

THE CATEGORY IS "UPHILL BATTLE"

3,500,000,000,000

$3,500,000,000,000.

What is the annual revenue loss due to fraud and financial crimes across industry in USD?

Source: www.ibm.com

SAD STATE OF SECURITY

"Many cyberattacks can be mitigated by relatively simple measures. Unfortunately, some people fail to take what appear to be basic precautions–such as using strong passwords, applying patches, and running a security solution. In many cases, breaking into a company's network is easier than it sounds."

Costin Raiu
Director, Global Research & Analysis Team
Kaspersky Lab

"I could teach a third-grader to do it."

Darren Martyn aka "PwnSauce"
LulzSec
After hacking senate.gov in 2011

The Current State of Cybersecurity is Not Nearly Good Enough, and is getting worse all the time!

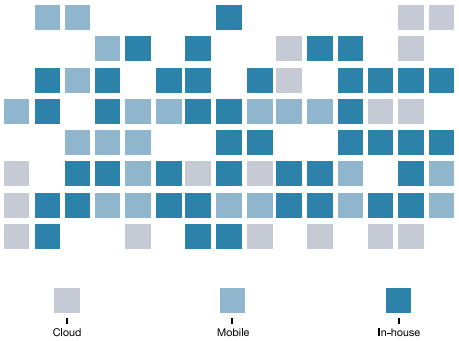
CENTRAL THEMES

- Breaches occur even in the most security conscious organizations
- Tenacity & skill of attackers when it comes to searching out weaknesses in organizations is unrelenting
- There is no substitute for a methodical and risk based approach to security management
- Your approach must address both the organization's security practices as well as downstream risk posed by vendors, suppliers & other third parties
- Know where your data is and how it *should* be classified!
- 90% of public breaches can be linked to an individual – so train well!
- All security begins with policy & policy is a statement of intent
- Measure your performance against a baseline standard: NIST CSF, NIST 800-53 & 30, ISO 27001/2

CYBERCRIME UNEARTHED

CYBERCRIME IS FLOURISHING

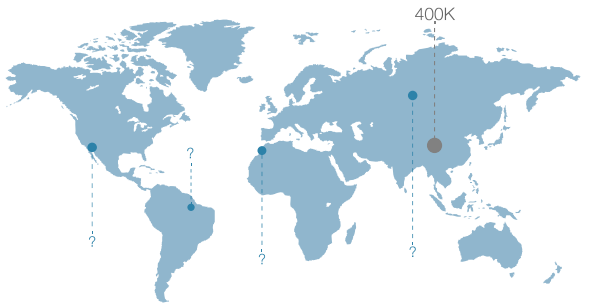
Expanding Attack Surfaces



Forbes, 2014

508 is the average number of applications in an enterprise

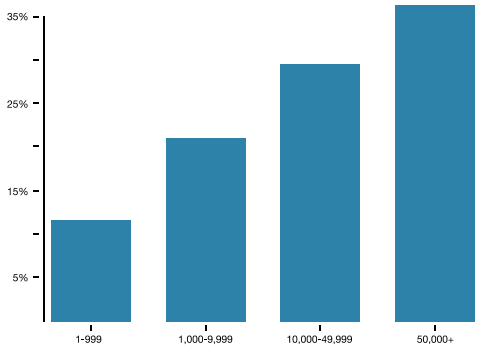
Evolution of Adversaries



AV-TEST, 2016

390,000 new malicious programs every day with a viable ecosystem

Overwhelmed Defenses



FireEye, 2015

37% of US companies face 50,000+ alerts per month

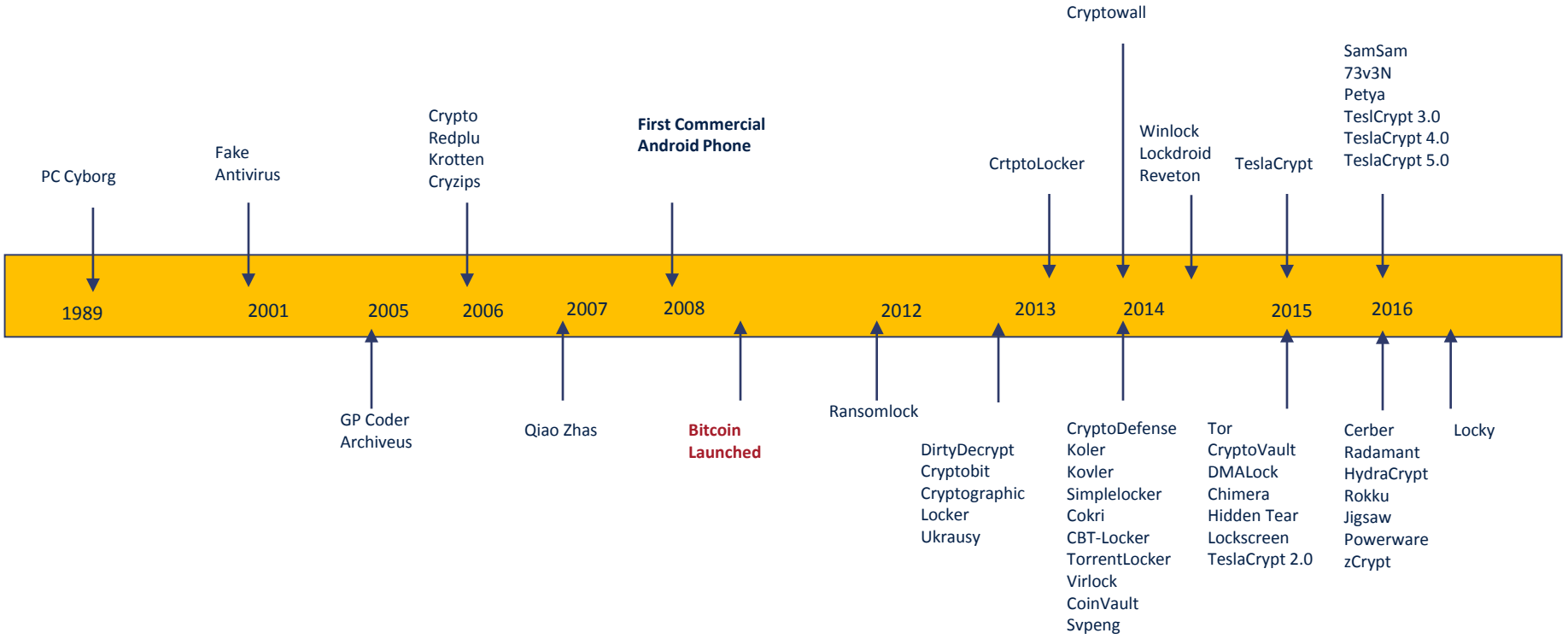
Source: Alert Logic

Source: Alert Logic

WHAT IS RANSOMWARE REALLY?

- Its malicious software!
- It requires you pay using the e-currency of the Wild, Wild Internet!
- It has 2 main flavors: *Locker* and *Crypto* (soon to be 3)
- Typical delivery occurs one of three ways:
  - Phished or spammed e-mail (most prevalent)
  - Malvertising
  - Exploit kits
- Ransomware variants families spiked by 752% in 2016

THE EVOLUTION OF RANSOMWARE



As you can see, its not new!

I can use Ransomware as a Service and keep 70% of the profit

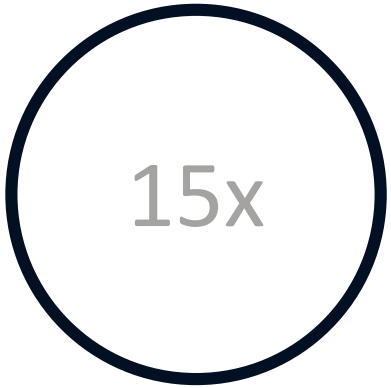
RANSOMWARE IS A MASSIVE MARKET

Size of the ransomware market CY 2016

Source: Federal Bureau of Investigation

$ damage 1H CY2017 alone!

Source: Cybersecurity Ventures



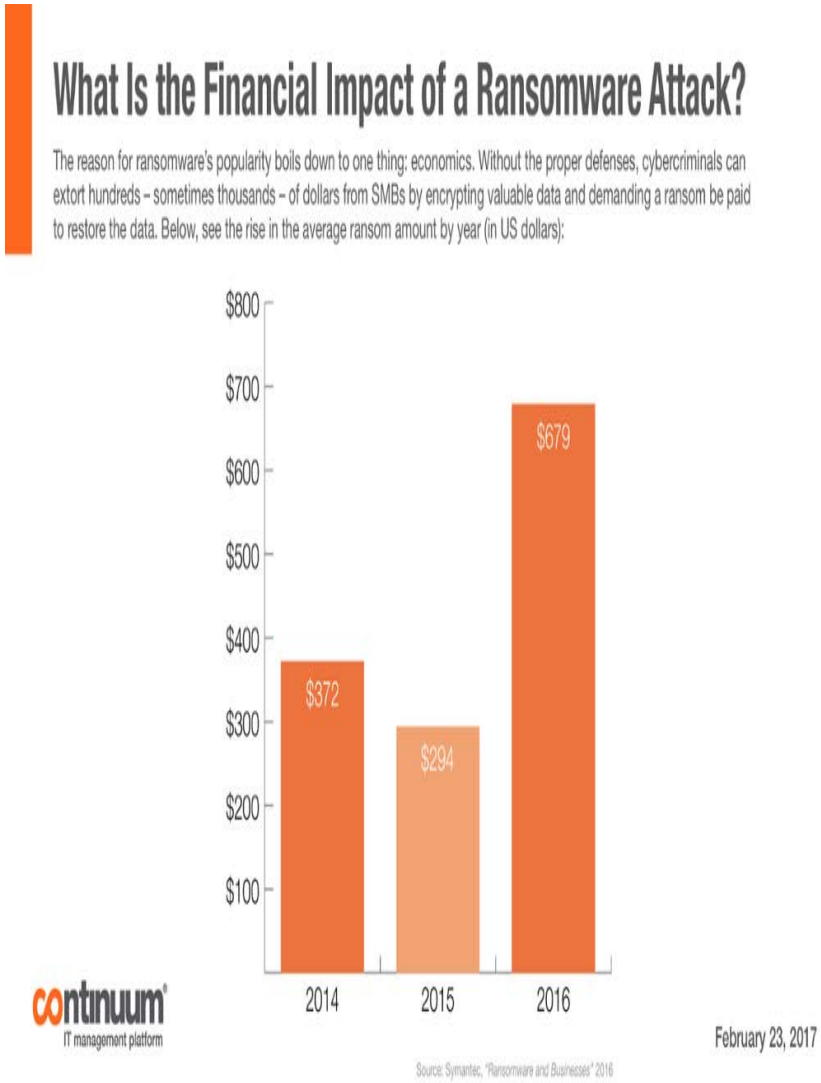
Damages up by 15x multiple in 2 years; will quadruple again for Healthcare by 2020

Source: Cybersecurity Ventures

RANSOMWARE BY THE NUMBERS

Economic Crime of Our Time

- 2017 US Business: <$5BN, up from $325M in 2015 (Cybersecurity Ventures)
- 4000 attacks per day on average
- $333,000 – Total recovery per ransomware incident (Trend)
- 433% ransomware attack increase YOY on SMB's (Kaspersky)
- 76% of ransomware comes from SPAM/Phishing (Kaspersky)
- 72% left organizations without access to data for >2 days
- 40% of victims pay the ransom (Osterman)
- 47% of all businesses in NA hit with ransomware in last 12 mos (Osterman)



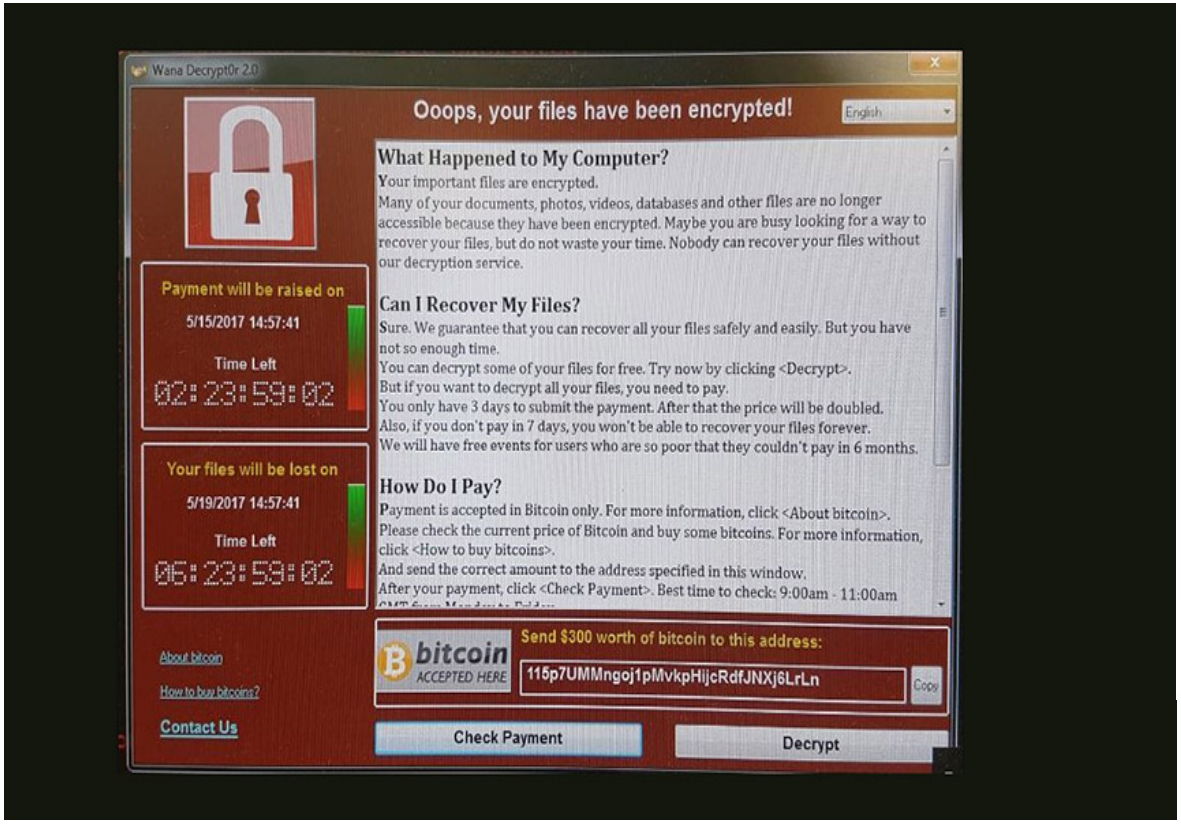
Avg. single ransom request in 2016: $679…Deceptive?

WHY WAS WANNACRY DIFFERENT AND MORE DANGEROUS?

- Many ransomware authors make “rookie mistakes” but not here
- WannaCry is well designed: 2048-bit RSA keypair on every machine
- Private Key is encrypted by author’s public key before stored
- Each *file* has its own AES key generated, that is then encrypted by the machine’s public key before stored
- You have 3 options:
  - Break RSA/AES
  - Pay the ransom
  - Restore from backup (hope you have taken and tested them)
- It’s a worm like MS Blaster and Conficker

Some benefitted by flaw in Windows API

WANNACRY RANSOMWARE

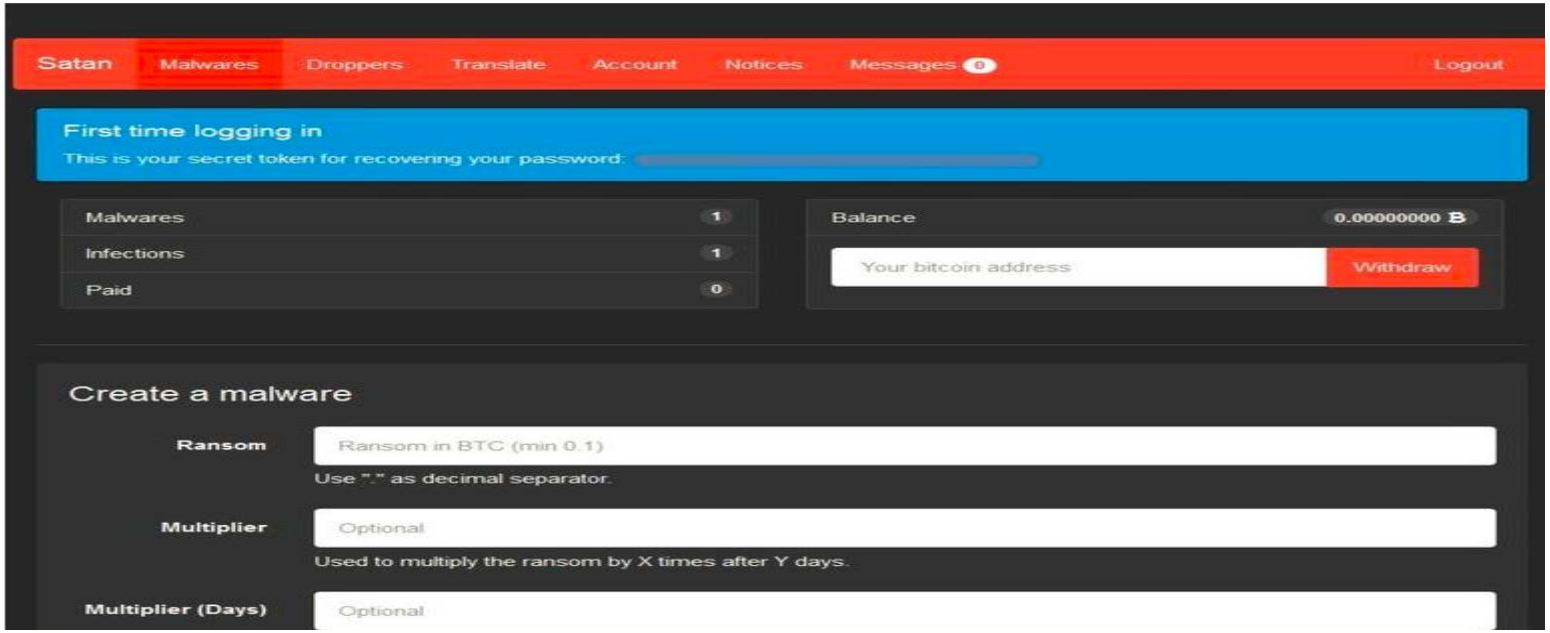


WannaCry Ransomware Variant with No Kill Switch Discovered
news.softpedia.com

Patching, A/V & Endpoint Admin Are Important But Insufficient!

Other higher order concepts are needed….

DARKNET & RAAS



- A.K.A. The Dark Web, Hidden Web, Deep Web
- Overlay internet that can only be accessed with privacy browsers
- The most common is the TOR (The Onion Router) Browser Bundle
- TOR was largely funded by the US government
- The Hidden Wiki – Censorship resistant wiki operating via TOR
- Every Fortune 500 company has some data exposure on the dark web
- Most sinister material on Internet is found here…it is dedicated to crime

It is the home of SATAN – Ransomware as a Service

TECHNOLOGY IS BOTH A CRIME ENABLER AS WELL AS INHIBITOR

Frank Abagnale: "Catching Me is Harder Now"

- Paying bills by check may cost you your savings!
- Abagnale: "We do little to protect consumers."
  - Few PSA's. Banks warn but in the form of a product, not a service
  - Grandparent's scam
  - Nothing stands in the way of copying your check details and forging them
- Committing financial crime today is 1000 times easier than it was 40 years ago
  - What took days, now takes milliseconds and can be done from 7,000 miles away

Anyone with a computer can say, "Who will my victim be today?"

THE IMPACT OF A BREACH IS FAR REACHING AND LONG LIVED

COMPANIES/INSTITUTIONS OF ALL SIZES ARE IMPACTED

THE CYBER KILL CHAIN[1]

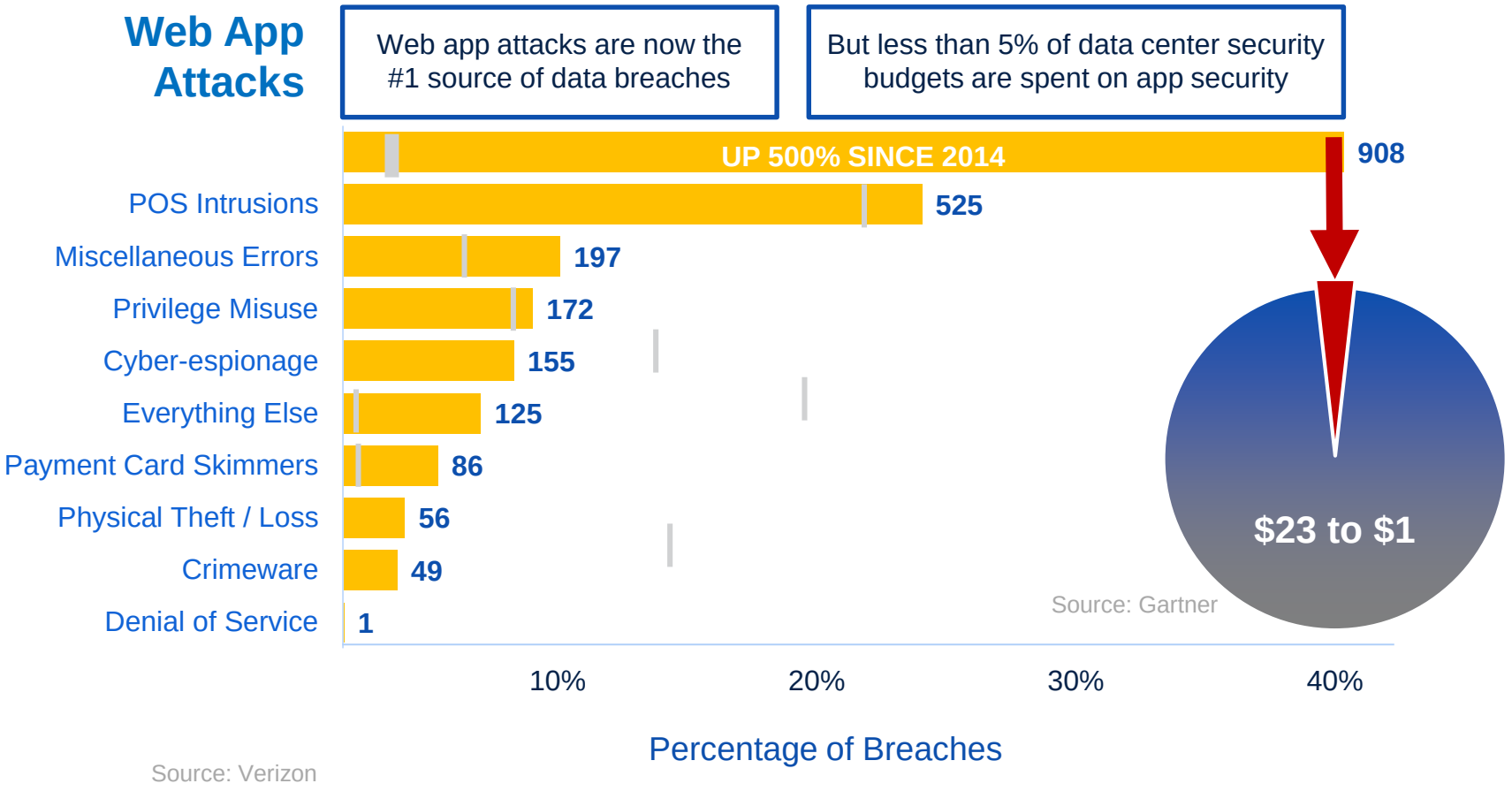
The Impact

- **Financial loss**
- **Harm brand and reputation**
- **Scrutiny from regulators**

Sources:

1) 2015 Cost of a Data Breach Study, United States, Ponemon Institute
2) CIO Today: Cost of Target Data Breach: $148 Million Plus Loss of Trust, August 2014
3) Reputation Impact of a Data Breach, Ponemon Institute, November 2011
4) 4 Reasons Why CIO's Lose Their Jobs, Silverton Consulting, Inc. StorInt™ Briefing,

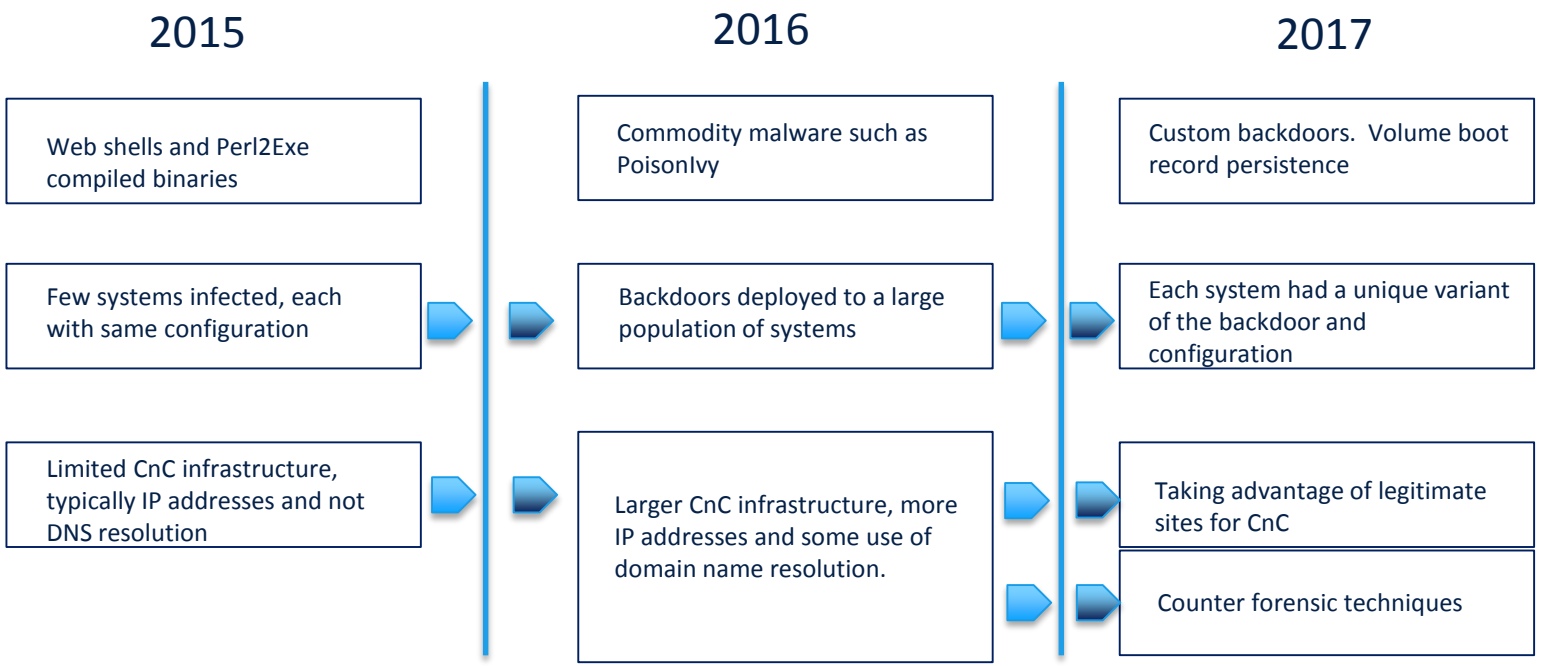
SECURITY RISK HAS SHIFTED TO “VALUE TARGETS”



Public Cloud sees fewer successful attacks than traditional or hybrid environments!

INCREASED SOPHISTICATION OF FINANCIAL ATTACKERS

- ✓ No longer do we see “smash and grab” attacks against ACH, PCI, tax returns etc.
- ✓ High levels of innovation and a relentless, motivated attacker, often nations state
- ✓ Attacker organizational hierarchy looks much like corporate America
- ✓ Bar now very high for defending against “hard to detect” attacks
- ✓ Attackers goal is now “residency” and long-term exfiltration



WHAT'S THE EQUIFAX SCORE?

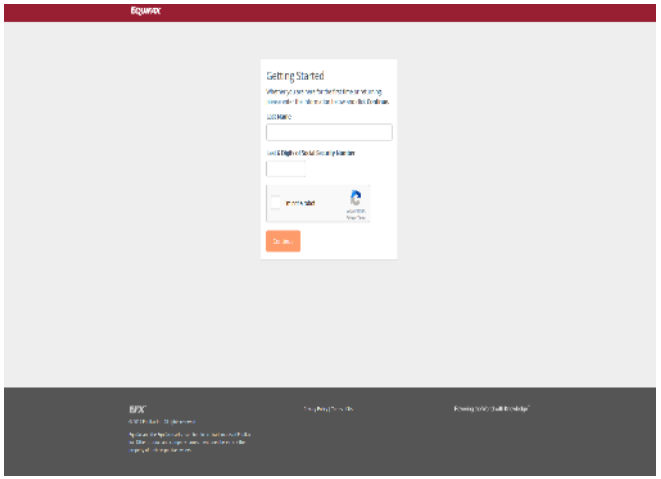
143~~3~~5 million US customers

- 44% of the population (really a lot more)
- SSN, DOB, DLN, Address, Full Name
- Your only solution is government regulation (and it pains me to say that)
- Open Markets will not fix this
- You are not an Equifax customer, you're its product
- 2500 to 4000 other data brokers collecting, storing & selling info on you (and you do zero business with them)
- These organizations do not answer to us
- Next massive breach will get us to forget about Equifax

“RING, RING….HELLO THIS IS EQUIFAX”

NO, ITS NOT….DO NOT TELL THEM ANYTHING

- This is just one scam we see right now
- Don’t trust caller id – spoofing is too good
- Hang up on all robocalls (don’t hit 1)
- Report fake calls to the FTC
- If its too late and you gave out info to an impostor:
  - Change passwords immediately
  - Report all affected accounts and have them blocked
  - Go to www.identitytheft.gov



One year of credit monitoring is akin to having an alarm system for one year!

DELOITTE SHOWS THAT “HACKERS GONNA HACK”, DATELINE 9/25/17

- CIA Triad: Confidentiality, Integrity, Availability
- I will tell you, integrity scares me more than the other two
- $37B firm
- Compromised emails and plans for blue-chip clients
- Attack went unnoticed for months
- Admin account gave the attacker privileged, unrestricted access
- Emails were stored in Microsoft Azure
- May have included architectural diagrams for at least six clients

They hired legal counsel in April of this year for “a potential cyber leak”

WHAT ARE FRAUDSTER'S UP TO?

MOBILE PAYMENT & TRANSACTION FRAUD

$721.4 T Market – Fraudster's Heaven!

- 78% of all merchants support mobile
- 40% feel mobile fraud is increasing
- 62% still use a 4 digit screen lock code
- Dark web: Credit cards - $1, Identities - $15; Online banking into - $300; Healthcare info - $350+
- To lower your risk as a merchant
  - Have a mobile app (15% can detect today)
  - Elude proxy servers – get real location
  - Determine if device is pre-paid
  - Conduct fraud audits once a year
- TEZ, Android Pay, Apple Pay, CapitalOne Wallet, Chase Pay
- Apple (61%) is most trusted, Android and Windows (least trusted, 3.7 and 1% respectively)

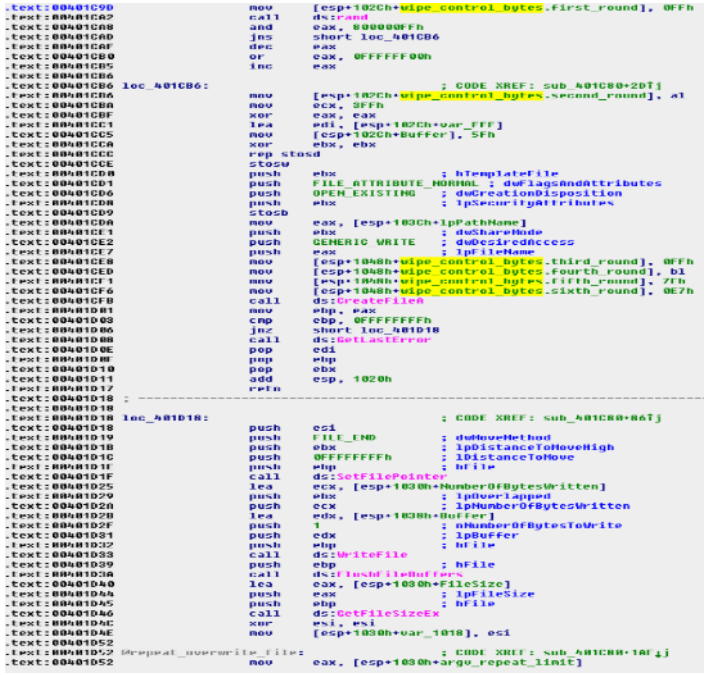
Facial recognition & MFA other schemes are the future of mobile payment technology, though many are rebelling against its use.

M-Security is here to stay but differs from E-Security & Requires New Measures

SWIFT ATTACKS OCCUR SWIFTLY

4 Major Attacks on Banks Using Swift in 2 Years

- Wells Fargo & Banco del Austro
  - 12 fraudulent transfer requests supposedly made to WF by BDA to move $12M in accounts to Dubai, US and Hong Kong
  - WF said it “properly processed the wire instructions received via authenticated SWIFT messages” and therefore isn’t responsible
- Evidence points to North Korea: It’s likely that the country’s Lazarus Group is responsible for the BCB (Bangladesh) attack and possibly other high-value SWIFT breaches.
- SWIFT argued that banks need to beef up network defenses, watch more carefully for fraudulent activity and always report any SWIFT-related issues.
- Banks, meanwhile, are calling on SWIFT to do a better job of protecting the system from malicious access



Unique wiping code found by security firm Symantec, in multiple attacks in Southeast Asia. Operation Blockbuster involved major security vendors sharing intelligence and resources in order to assist commercial and government organizations in protecting themselves against Lazarus.

EVASIVE ACTION AGAINST CYBERFRAUD

Innovation by malware authors

- File encryption and virtual machine awareness inhibits countermeasures
- Installs lightweight Linux OS, deletes your security software upon reboot, and then fires Windows again, with no protection
- Rootkits, and infected master boot records
- File watchdog processes to initiate downloads when initial malware is deleted
- Social: Mass & Targeted; Wangiri Fraud, Pretexting, Phishing, CEO, Lottery, Telecom, Baiting, Chattel Diversion

- Not illegal to hack outside Russia
- Not illegal to *modify* your name…Joseph G. Vigorito can become Geo Vigori
- Anyone can set up a ghost address (Spain) linked solely to your email…essentially all anyone knows is that you are on earth (protonmail, tutanota)

SO WHO PROTECTS THE PUBLIC AT-LARGE?

CONSUMER FINANCIAL PROTECTION BUREAU

- Goal of stamping out illegal and predatory practices
- Created 7 years ago in wake of financial crisis
- $12B in relief for 29 million harmed
- Who do they offer consumers protection from?
  - Banks, for opening NOW and credit card accounts with authorization; charging overdraft fees without consent
  - Credit card companies for unfair and deceptive practices
  - Mortgage companies for wrongful foreclosure
  - Debt collectors for illegal intimidation tactics
  - Student loan servicers for illegal servicing practices
- Handles 1.2 million complaints
- Perhaps most importantly, they banned use of arbitrations clauses that disallow consumers to have their cases heard in courts of law
- Bottom Line: CFPB is under jurisdiction of Federal Reserve and may get disassembled or realigned

www.consumerfinance.gov

Does the CFPB do enough vis-à-vis $3.5T loss?

DHS IDENTIFIES 21 TARGETED STATES IN 2016

If it touches the internet, it can be hacked

- Voting machines are not connected to the internet but those housing voter rolls and logs, usually are
- Hacking is not the same as voter fraud…yet
- Illinois, Arizona can point to hacker entry
- Some of other 19 might have data exfiltrated
- One “white hat”, Chris Grayson, was able to penetrate the State of Georgia and download confidential voter files of every Georgian
- No evidence of tampering with vote tallies exists
- In California, phished emails were used to trick an employee into revealing their login to systems that track voter eligibility in 8 states

Who protects the voter? Election Assistance Commission (EAC) – Being done away with…..*What?*

What the internet did for communications, blockchain will do for trusted transactions.

-Ginny Rometty, CEO of IBM

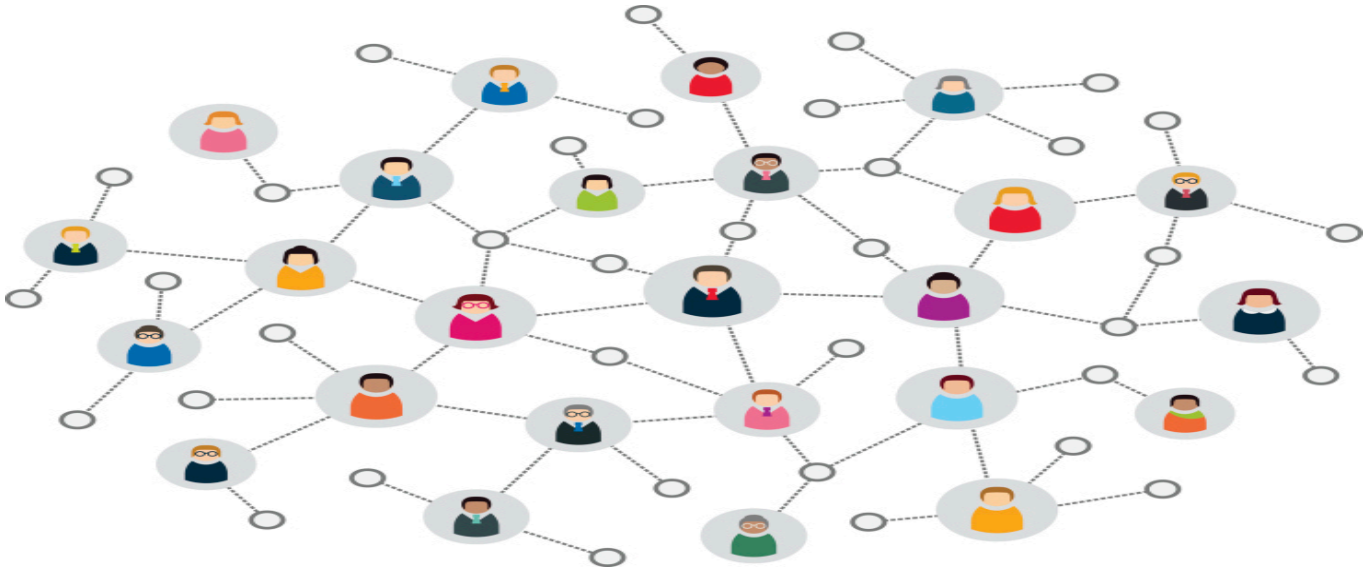
WHAT IS BLOCKCHAIN?

It is a “value network based on the Internet”

- Real time ledger of anything you can record:
  - First created to track Bitcoin transactions
  - Financial transactions, contracts, diamonds, physical assets, supply chain info, etc.
  - No single person “is in charge” of the “chain”
  - A “block” is the detail of each record; blocks can be owned via a private key held only by that owner
- Every block is time stamped and encrypted
- When the owner makes a change to a block, the members of the chain see it in realtime, no middle man! True peer to peer system
- Ex. A blockchain stock purchase settles in minutes; no T+3
  - Every transaction goes into a block and each block connects to its predecessor and eventually its successor; each block contains a crypto copy of its predecessor, making it immutable

Overstock.com issues its equity on a platform powered by blockchain, t0.com, an integrated cryptographically secure distributed ledger that reduces costs, increases transparency, efficiency and auditability.

IS BLOCKCHAIN THE IDENTITY PANACEA?



- Ex. Unique identifier and DOB to prove you are over 21 or your credit score and ID at a bank to prove credit-worthiness
- Notion of self-sovereign identity by imparting only what is needed at that time
- Distributed nodes element is interesting, but every node has a copy of everything, making the notion of trusted identity challenging

IBM, Apple, Microsoft, Facebook, Amazon all have Blockchain researchers

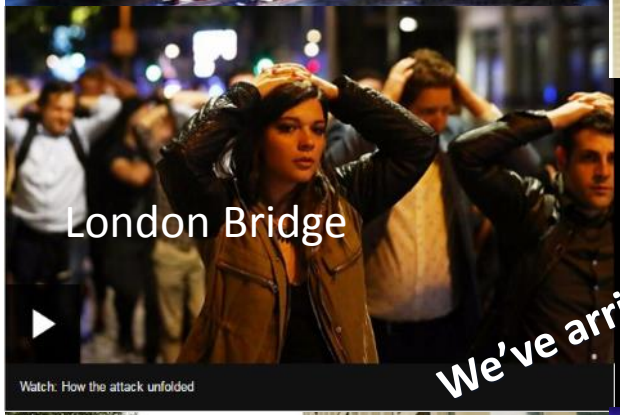
THE IMPACT IS PERVASIVE AND CATASTROPHIC

DOWNHILL SLIDE

STUXNET VIRUS

Cyberweapons are now very much in play!

DOWNHILL SLIDE

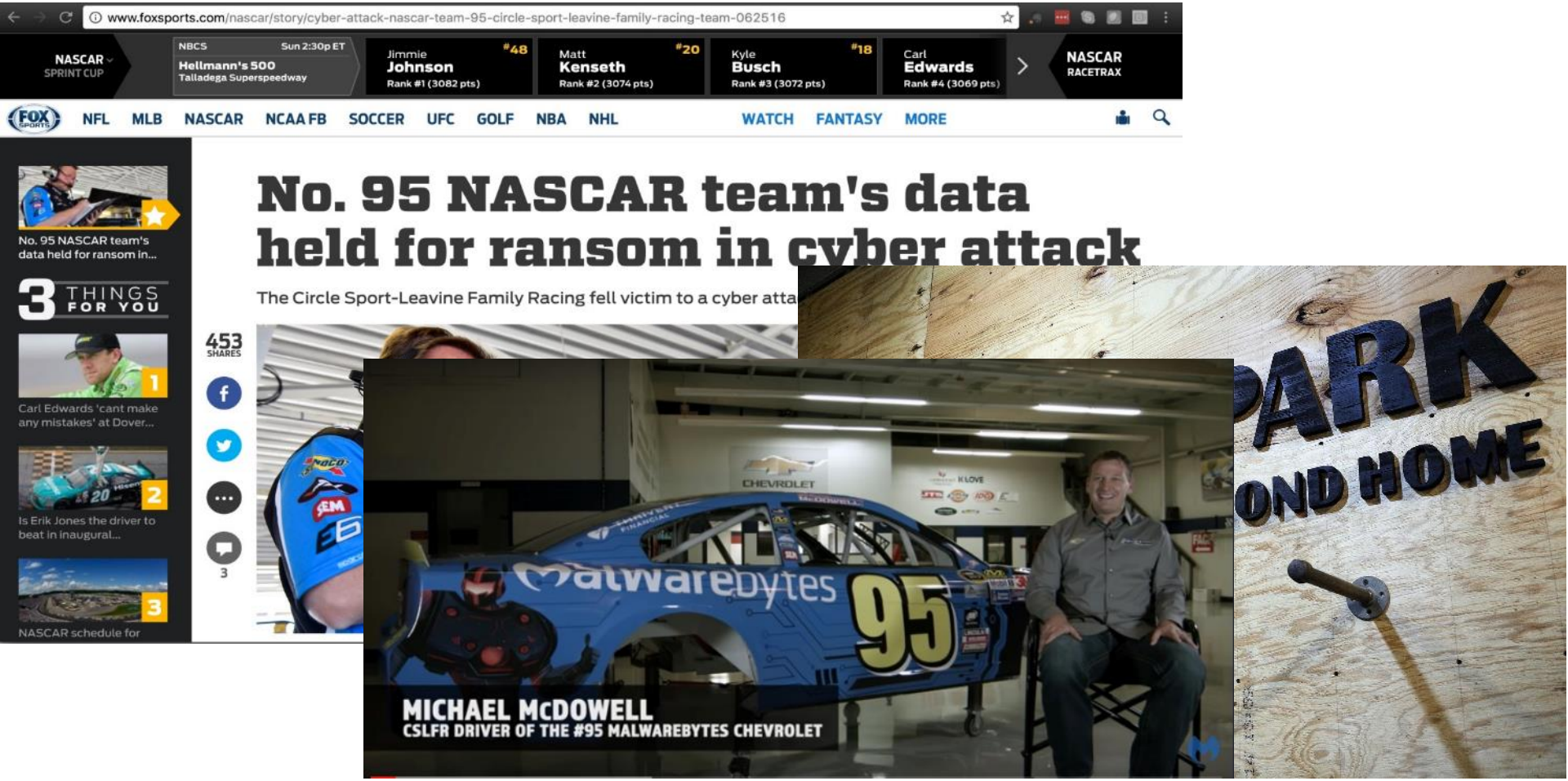


We’ve arrived at the Nexus of Terror and CyberTerror

Cyberweapons and Terror Weapons Now Serve Cross Purposes

WHO GETS TARGETED? BIG

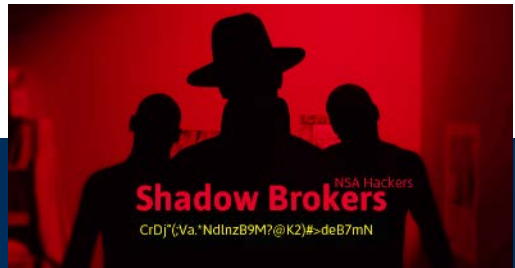
WHO GETS TARGETED? AND SMALL



AGE OF THE PERFECT RISK STORM

EVOLUTION OF THE ATTACKER

- Moving from hacktivism in social context to the political context (Operation Avenge Assange & Operation Egypt)
- They move across the globe in seconds
  - There is no need to compromise a machine in North Korea, when I compromise a machine in Russia that is already attacking a machine in North Korea.
- They are often well-funded, organized, committed to the cause; they have HR recruiters, tech support, benefits packages, legal representation and they get reviewed.
- They can launch full scale global DDOS attacks at any time, and likely have control of thousands of command and control botnets at this moment.



OTHER RECENT EVIDENCE

- Yahoo! – Perpetrator unknown. 500 million accounts in Sept. '16, 1 billion in December. User names, email addresses, date of birth, passwords, phone #'s and security questions leaked
- Mark Zuckerberg Hack – OurMine Group. His Pinterest and Twitter accounts were hacked multiple times because he used the password 'dadada'
- Oracle Micros Hack – Russian hacking group known for hacking banks compromised Oracle's POS system code on one of the top 3 payment card systems globally
- Russian interplay during Presidential election season – large scale phishing campaign to harvest emails which were then published via various sources including, purportedly, those from Wikileaks
- French election in May – Russian hackers, undetected by ANSII, compromised French infrastructure and released info to social media 36 hours before Macron election

These are just the ones your are hearing about!

"You can't defend. You can't prevent. All you can do is detect and respond." – Bruce Schneier

MORE RECENT SAMPLES

It Keeps Getting Worse for Dying Sears, Now Kmart Was Just Hacked

Brian Sozzi | Follow | Jun 1, 2017 7:40 AM EDT

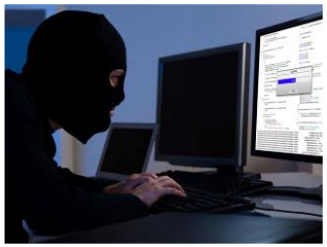
US intelligence director warns of more Russian cyber attacks

BY AP | UPDATED: MAY 11, 2017, 10.37 PM IST

Post a Comment

WASHINGTON: The director of national intelligence says Russia and other countries, including China, North Korea and Iran, are using cyberspace to target US and its allies, and will do so in future.

The Senate intelligence committee is holding a hearing on worldwide threats, and intelligence director Dan Coats says Russia is a threat to US government, military, diplomatic, business and critical infrastructure.



US intelligence director Dan Coats says Russia is a threat to US government, military, diplomatic, business and critical infrastructure.

Get ready: More cyberattacks are coming

Updated 1 hour ago

Top news

Businesses are bracing for a resurgence of a global ransomware attack already affecting more than 200,000 computers, when workers log back on this week. Experts warn that the "kill switch" ound in the malware on Saturday by a British

Phishing scam diverts more than $40,000 from Denver Public Schools

POSTED 9:33 PM, APRIL 5, 2017, BY MICHAEL KONOPASEK

LAW & JUSTICE

Newark City Hall computers hacked with ransomware

By MARK J. BONAMO
April 24, 2017 at 4:19 PM

87

NEWS

13

Uploaded: Thu, Apr 20, 2017, 3:41 pm

British Airways IT failure caused by 'uncontrolled return of power'

Cause of outage has not been revealed but BA says it was not due to an IT shutdown and was not linked to job outsourcing

PAUSD student data exposed in breach

'White hat' security researcher accesses school records

April 6, 2017 by Adam Harris

Breach of Financial-Aid Tool May Have Compromised Data on 100,000 Taxpayers

Nearly 100,000 taxpayers may have had their personal information compromised by a security breach of an Internal Revenue Service tool that makes it easier to fill out the Free Application for Federal Student Aid, the Fafsa, according to the IRS commissioner, John Koskinen, who testified on Thursday before the Senate Finance Committee.

JUST THE PAST 180 DAYS!

Hackers recently absconded with 1.5 terabytes of data from HBO, and have since leaked unaired episodes of *Ballers, Room 104,* and *Game of Thrones. Attack on Windows & individual employees.*

78 million of its customers have had their user account details stolen usernames, email addresses, and hashed passwords were taken from the service and have been put up for sale on the dark web for around $1,000 (£700).
.

Kromtech Security Research Center discovered a new Verizon leak exposed confidential data on internal systems. Leaked data includes server logs and credentials for internal systems found on an unprotected Amazon S3 bucket. The archive refers to internal Verizon Wireless systems used by the company to deliver data from the back-end systems to the front-end applications used by employees and staff.

Israeli security company Cellebrite was linked to the FBI's hacking of the San Bernardino terrorist;s iPhone 5C. It's been revealed that *Motherboard* was sent 900GB of the firm's data including customer information, internal databases, and technical data on the company's mobile phone hacking products.
.

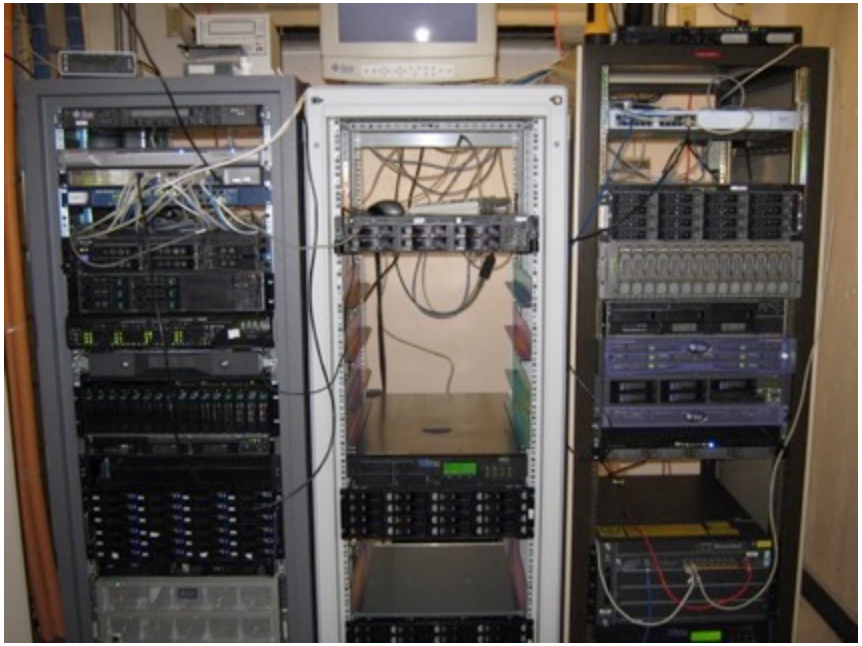
UpGuard has recently discovered a wide-open, public-facing misconfigured Amazon Web Server S3 cloud storage bucket containing roughly a gigabyte's worth of credentials and configuration files for the backend of dozens of Viacom properties.

Major companies, 5-7 years behind the cyber curve. The list is nearly endless!

QUO VADIMUS?

INFRASTRUCTURE HAS CHANGED

Buying Hardware

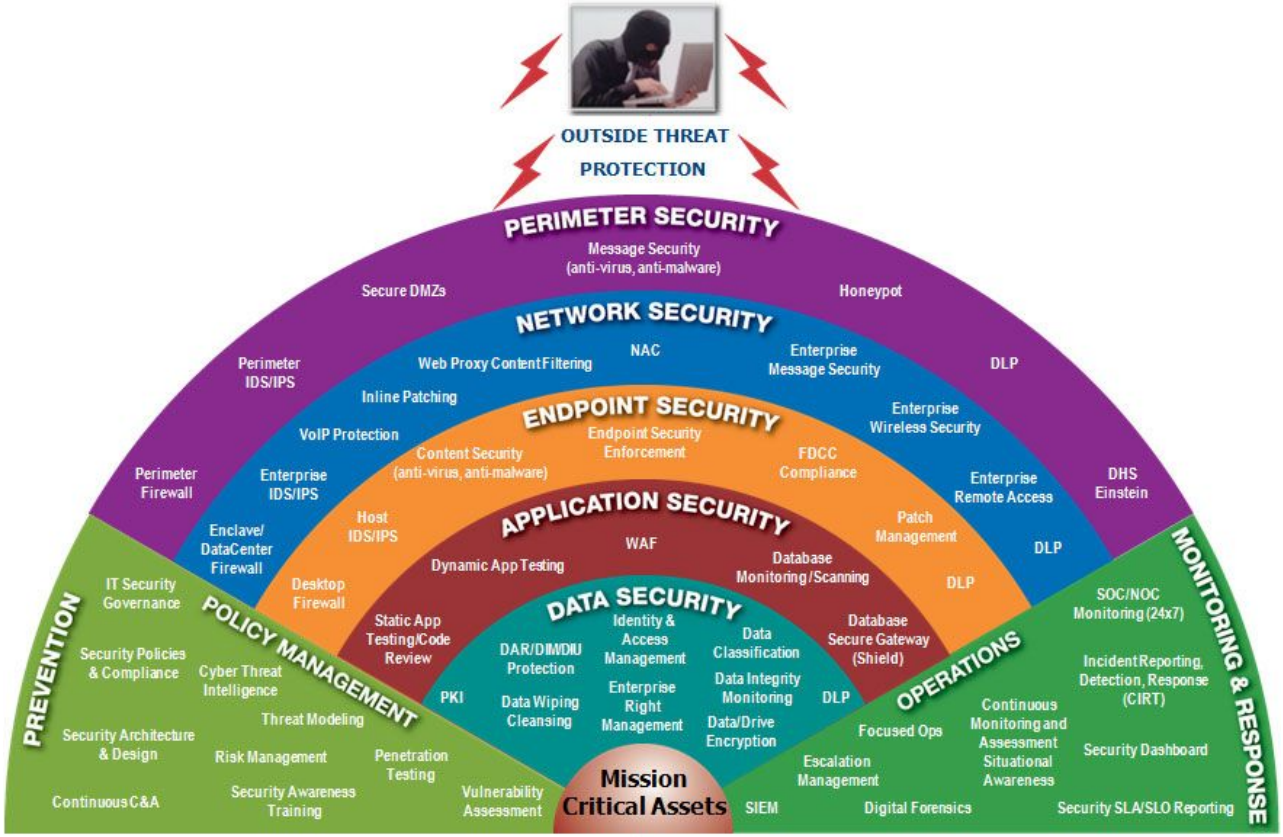


Infrastructure As a Service

EARLY 2000's → MID 2000's → NOW

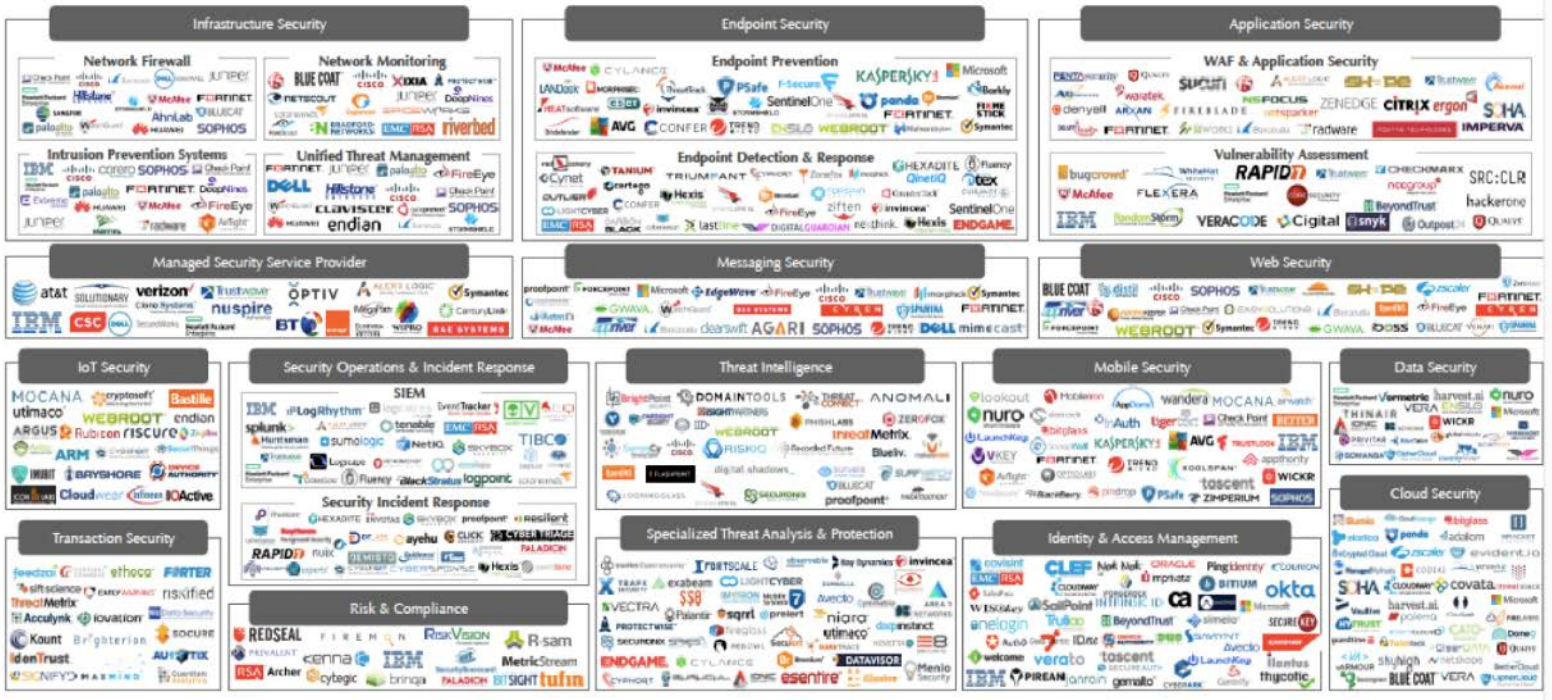
The one on the right can be bought with a credit card!

SECURITY HAS CHANGED AS WELL



Source: Alert Logic

SECURITY HAS CHANGED



Source: Alert Logic

LASTLY CYBERCRIME HAS CHANGED

Single Actors

EARLY 2000's | MID 2000's | NOW

LASTLY CYBERCRIME HAS CHANGED

Single Actors

Highly Organized Groups

EARLY 2000's → MID 2000's → NOW

Anonymous, LulzSec, Cyberzeist, Cult of Dead Cow, Shadow Brokers, etc.

NEW WORLD ORDER 2017

Business disruption attacks

- Destroy critical business data
- Combined ransom & leakage of confidential data
- Taunt executives / board members

NEW WORLD ORDER 2017

Business disruption attacks

- Destroy critical business data
- Combined ransom & leakage of confidential data
- Taunt executives / board members

Extortion to join the network

- New SPAM campaigns
- Pass on the malicious URL and infect others
- Infect 2 others and receive the decryption key

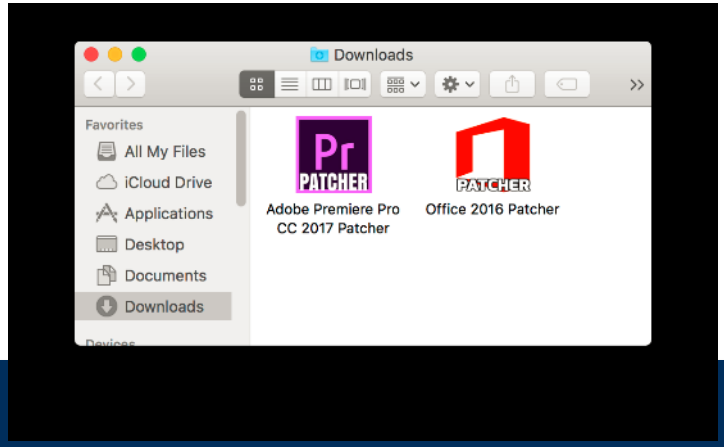
NEW WORLD ORDER 2017

Business disruption attacks

- Destroy critical business data
- Combined ransom & leakage of confidential data
- Taunt executives / board members

Extortion to join the network

- New SPAM campaigns
- Pass on the malicious URL and infect others
- Infect 2 others and receive the decryption key

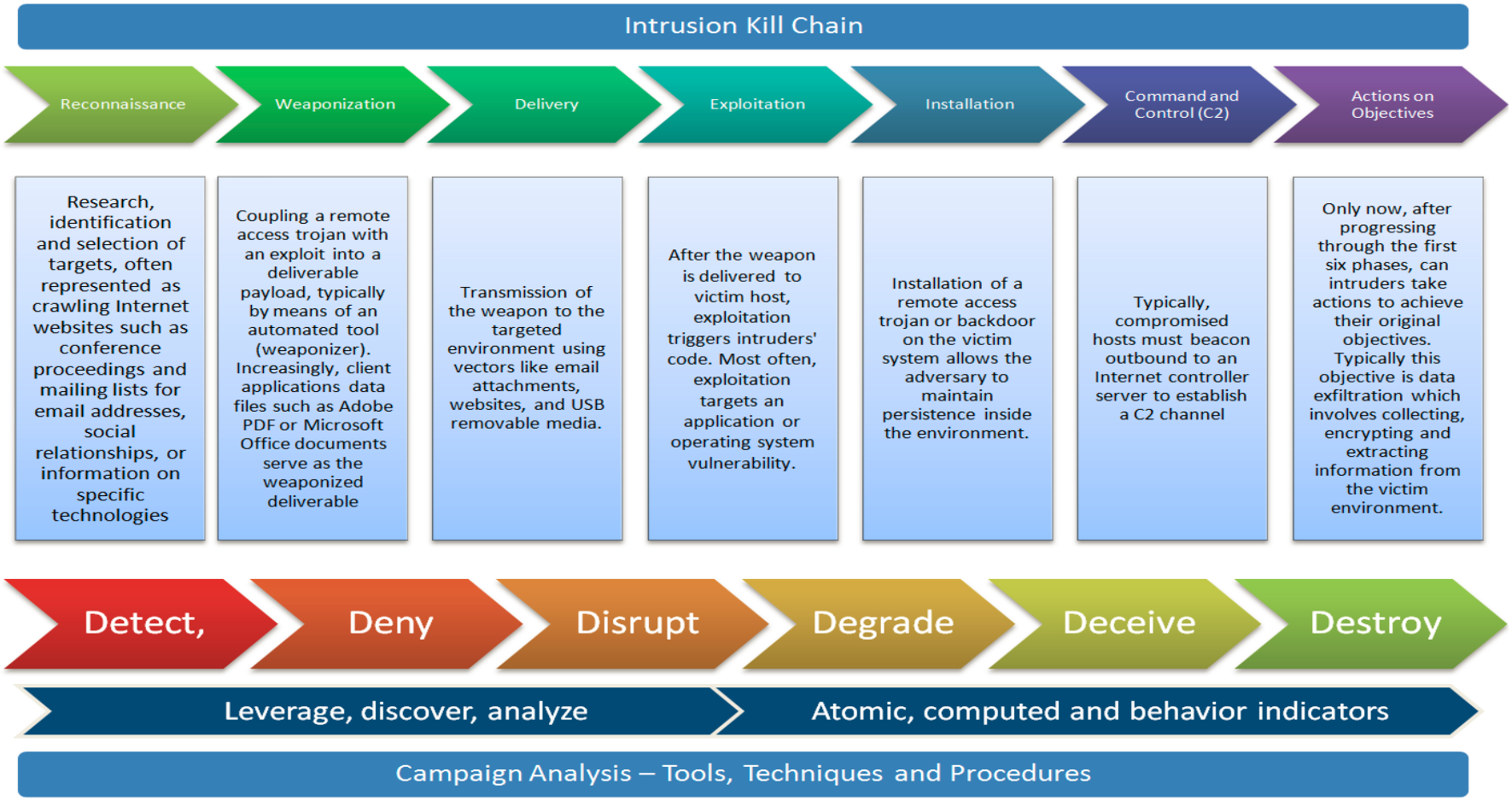


New Masqueraders – Patcher (3/17)

- Pretense of being a patching tool for Office running on MacOS
- Inexperienced authors have broken command and control
- Even if you pay, you will never receive the decryption key

SO WHAT? NOW WHAT

TODAY'S ATTACKS HAVE SEVERAL STAGES



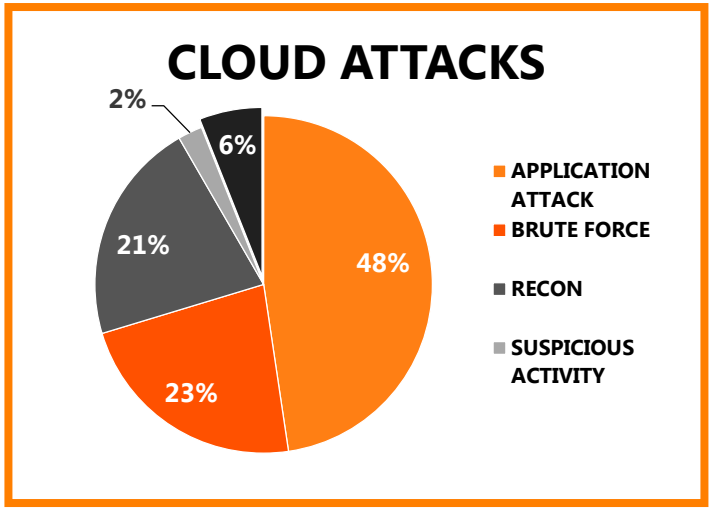
2017-2020 ATTACK PALETTE

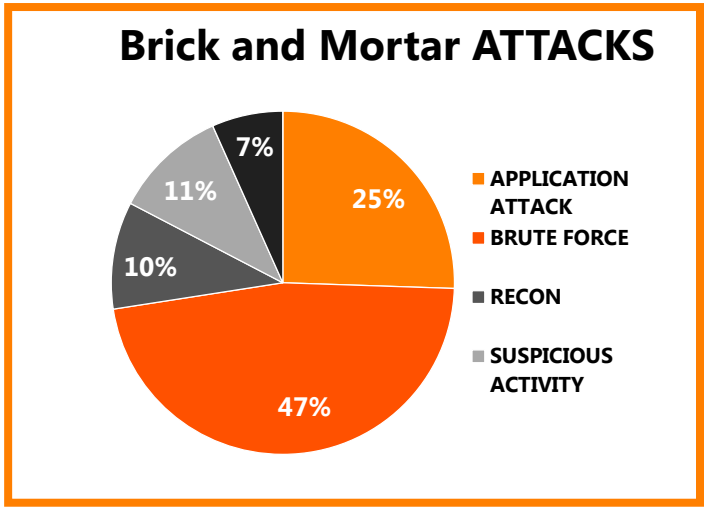
Nation State Cyber Attacks	Evolution of Ransom-ware-Worms, RaaS, "Victim as Extorter"	DDOS attacks will grow in size with planned targets	IoT attacks will replace "grid" based exploitation	Social Engineering and Insider leveraging will still be weak link	Business Disruption implies data destruction rather than encryption	Attacks on infra-structure will move forward in the cyber kill chain	Increas-ed attacks on iOS and Android

- GAO reports a 13-fold increase in attacks on 24 agencies over 10 years
- Russia's aggressive actions will continue: capable, funded & committed
- US-CERT: 4,000 attacks daily in 2016 (4x 2015)
- RaaS opens door to the unsophisticated and criminal element
- OVH and Dyn (Fall 2016) victims of Mirai
- Volume, Protocol and Application Layer
- 55% of all attacks are carried out with the help of malicious insiders
- More malware-less attacks: Powershell, Scripting, Memory

ATTACK METHODS ARE EVOLVING

- Security risks
  - Perception of increased risk due to lack of control
  - Blind spots: no way to connect on-premise and cloud attacks
  - Increased threat surface
  - Tuning tools for relevant notifications





Source: Alert Logic CSR 2016

WHY INVEST TO PROTECT? *COST OF A DATA BREACH IN 2017*

- June 2016, Ponemon Institute polled 63 US companies, 16 industry sectors
  - Average cost per data breach was $7.35M USD, up from $7.0USD in 2016 (up 5%)
  - Average cost per stolen record was $225,USD up from $221 USD in 2016 (up 2%)
    - FinServ data breach costs are $336 per capital, second highest to Healthcare ($380 per capita)
- Average number of breached records is 28,512
  - 47% of attacks are classified as malicious or criminal attack and cost $156 per record
    - This means 53% are system error, negligence error and cost $126 to $128 per record
  - Time to identify and time to contain are highest in malicious and criminal attacks (191 and 66 days respectively)
  - Encryption and incident response teams can reduce stolen record costs from $156 per record to $142 per record
  - Certain industries are more vulnerable to churn: FinServ, Life Sciences, Health, Tech, Service

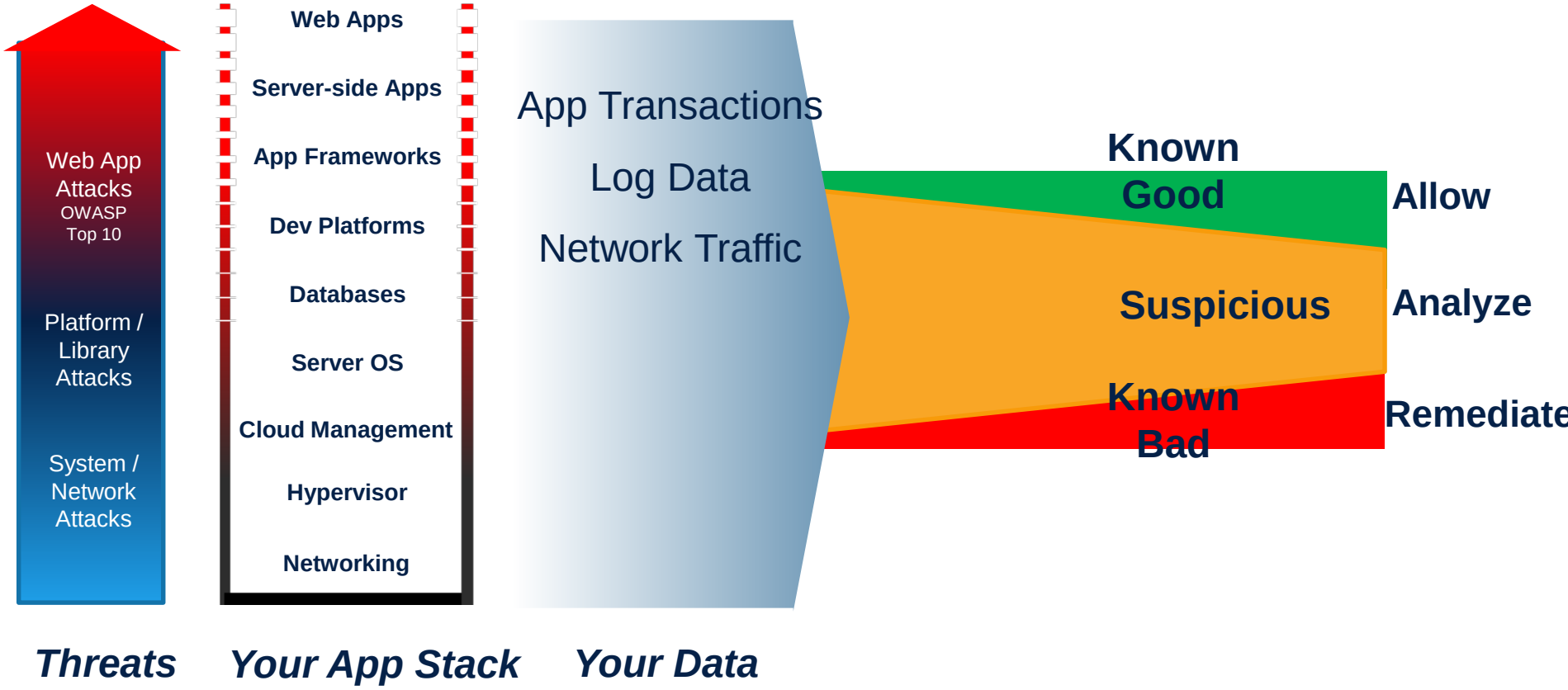
While there is no guarantee against being breached, tools & techniques such as advanced firewalls, AI based endpoint protection, encryption, least privilege, vulnerability and threat management, and data loss prevention, added to good governance, awareness and identify lifecycle management, go a long way towards mitigating risk of such events

POLICY, PEOPLE, PROCESS, PREVENTION = SUCCESS

THE HIGHER ORDER OF SECURITY

- Prevention
  - Modernize your security capabilities
- Data Classification & Information Impact
  - What data does my organization need to function and where is it?
- Business Resiliency / Continuity
  - Can I operate if every tool currently at my disposal is impaired?
- Incident Preparedness
  - Canary in the coal mine test: If staff sees a ransom note, they do what?
- Detect/Respond Compliments, *Not Replaces,* Prevention
  - Threat or Breach Hunting Tools/Skills are Key

PROTECTION NEEDS TO BE FULL STACK WITH COMPLEX ANALYSIS



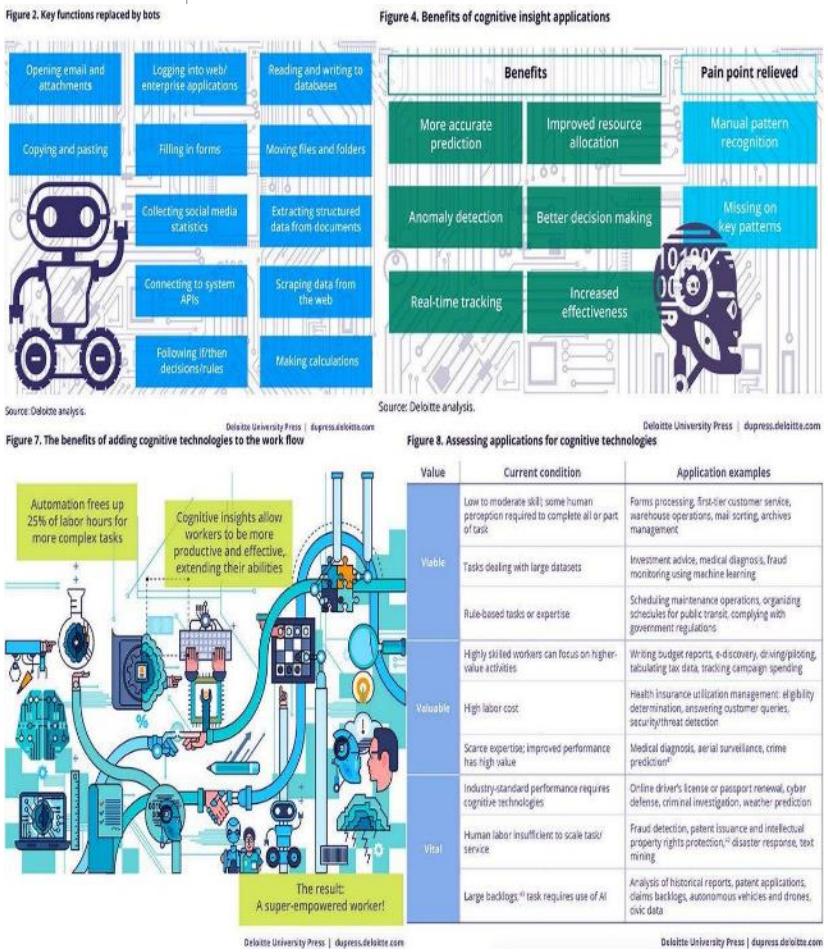
FIREWALLS AND ANTI-VIRUS WILL NOT CROSS THE RUBICON

- Guardrails > Gates (less control friction)
- Cyber Network Attack (greater “ground truth”)
  - Cyber Network Exploitation
- Higher the best people you can find who are “cyber curious”
- Implement continuous cyber-awareness programs
  - Point in time are not enough
- Stay laser focused on People, Policy and Process (tools are not enough)
- More automation = less human error
- Have a patch approach – don’t set a policy you can’t a
- AI/ML are NOT the future, they are the present!

ARTIFICIAL INTELLIGENCE

Answer to the Cyber-Hacking Threat

- What level of monitoring and activity reporting are you willing to live with?
- AI emulates the ideal human condition
- Quickly and accurately identify what is safe and what is a threat
  - Not just whitelist or blacklist processes
- Sophisticated math combined with unique understanding of hacker mentality



AI is a powerful tool that balances security and privacy (and will be used by hackers too)! It is simpler, smarter security.

TAKING THE POLITICAL TEMPERATURE

PRESIDENTIAL EXECUTIVE ORDER

- May 11, 2017 (oddly, one day before WannaCry)
- 3 Directives:
  - Protect Federal Networks using the NIST Framework (the CSF)
  - Mandate Federal IT move to the Cloud
  - Centralize Federal IT as one enterprise network
- 4 Elements:
  - Vulnerabilities: A full US review shall take place immediat
  - Adversaries: A full identification will take place within 90 days
  - Capabilities: NSA, DoD and DHS will be evaluated
  - Private Sector: Commerce and DHS will have 120 days to report

Heads of each agency are responsible for cyber

DIGITAL GENEVA CONVENTION

- Microsoft make call again after releasing patches for unsupported XP in wake of WannaCry
- "…this attack provides yet another example of why the stockpiling of vulnerabilities by governments is such a problem."- Brad Smith, Microsoft President
- Commits governments to protect civilians from nation-state attacks

YOUR MONEY OR YOUR DATA: SHOULD YOU PAY A RANSOM?

- We never recommend payment
- We recommend preparation
- Ransomware is often downloaded with an Advanced Persistent Threats
- Just like DRP Planning, use Business Impact Analysis documents
- If you have cyber-insurance, don't just assume you can claim ransomware
- Pay only as a last resort but negotiate the price!
- Talk to your banker(s) about bitcoin, know how to exchange
- Use continuous learning tools (Wombat or KnowB4)
- Implement application whitelisting and content filtering
- Use 3-2-1 rule for backups
- Have a CMDB and be able to host re-image quickly

Use concept of "zero-trust"

23 NYCRR 500 – DFS

- These are foundational functions, not surprises
- Assess your current risk profile
- Design a methodical program that addresses risk
- Senior Management is Responsible!
- Senior Management will file an annual certificate of compliance
- CS Program ensures the safety, the soundness of the institution and protection of its customers

23 NYCRR 500 KEY DATES

- August 28, 2017 – 180 day transitional period ends. Covered entities must be in compliance
- September 27, 2017 – Initial 30 day period for filing notices of exemption under 500.19(e) ends on or prior to this date
- February 15, 2018 – Covered Entities required to submit their first certification in accord with 23 NYCRR 500.17(b) on or prior
- March 1, 2018 – One Year transitional period ends. Need to be in compliance with sections 500.04(b), 500.05, 500.09, 500.12, 500.14(b)
- Your policies should include data governance, data classification, asset inventory and device management (4 key policies)

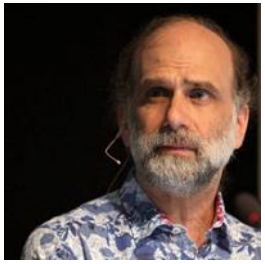
GENERAL DATA PROTECTION REGULATION

- Currently called DPA (Data Protection Act) – Approved 4/2016
- Applies to anyone with employees in EU or doing business in EU
- Focused on PII
- **Penalties and fines can be 4% of global revenue!**
- GDPR bestows client control over personal data, to modify, restrict, withdraw or transfer
- Walk into Apple and tell them to transfer iTunes to Spotify!
- Concept of Unified Governance: HIPAA and GDPR have similar goals
- May 25, 2018 deadline – opportunity to secure competitive advantage (in theory)
- Disruptive!! Not like SOX, HIPAA or PCI at all – data minimization rule for example.
- Business imperative and a business problem, not a pure-play compliance issue!
- Requires a GDPR Readiness Assessment or Gap Analysis

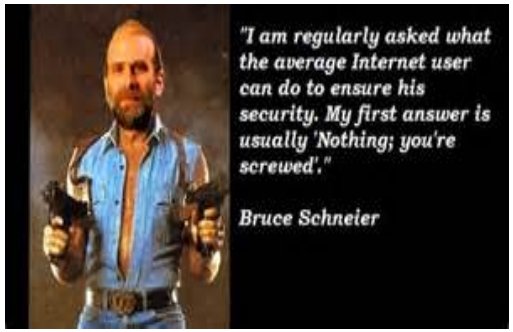
TIME FOR CHANGE IS NOW

FEELING BETTER YET?

Peiter C. Zatko, better known as Mudge, was a member of the high profile hacker for the group L0pht. **He was testified before a Senate committee in 1998 that they could bring down the Internet in 30 minutes**



"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology." - Schneier



Dan Kaminsky discovered the Internet wide DNS Cache Poisoning Vulnerability in 2008. "I do not need to hack you. I just need to hack someone who has already hacked you."

I GET HIRED BY COMPANIES TO HACK INTO THEIR SYSTEMS AND BREAK INTO THEIR PHYSICAL FACILITIES TO FIND SECURITY HOLES. OUR SUCCESS RATE IS 100%; WE'VE ALWAYS FOUND A HOLE.

- KEVIN MITNICK

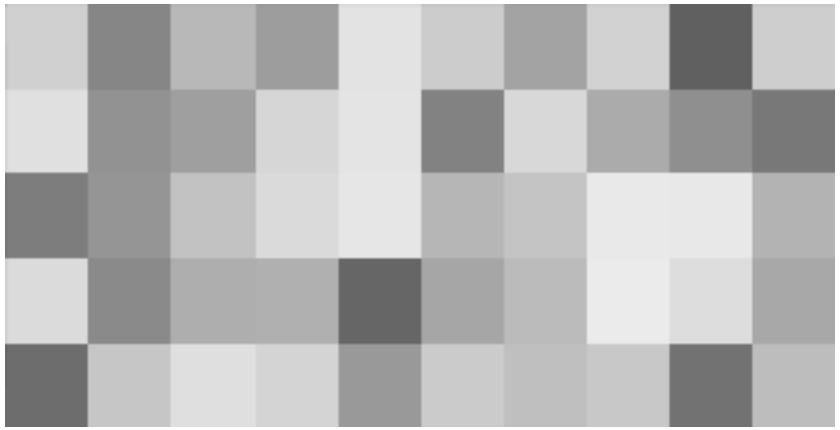
QuotePixel.com

"PERFECT" IS NOT THE ENEMY OF "GOOD"

- Perfection rarely happens in security, be "good" and "get better"
- Breaches happen in the most security conscious organizations
- Layer – Defense in depth (perimeter, network, host, app, data)
- Limit – Compartmentalize, limit access and permissions
- Obscure – Hide your assets; encrypt your own; consider intelligent deception tools (decoys)
- Diversify – Use a variety of techniques; suppliers; tools; monitors
- Simplify – Have a simple set of policies that everyone can understand but remember the 4 you need:
  - Information Protection, Data Classification, Data Governance, Incident Response and Business Continuity

CONVENIENCE/SPEED VS. PROTECTION/CONTROL

CYBER LIVES IN SHADES OF GRAY!



You cannot fix every security problem all at once.

Do a methodical, precise risk assessment.

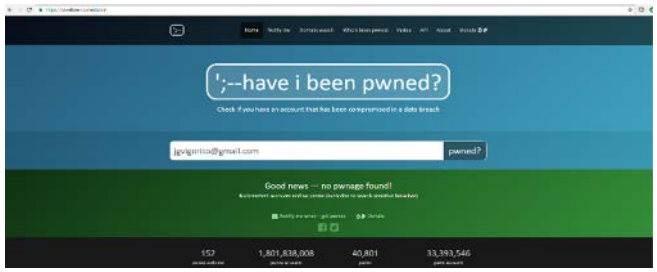
Measure that risk against "cost" of attendant controls.

Implement, then test regularly. Be accountable.

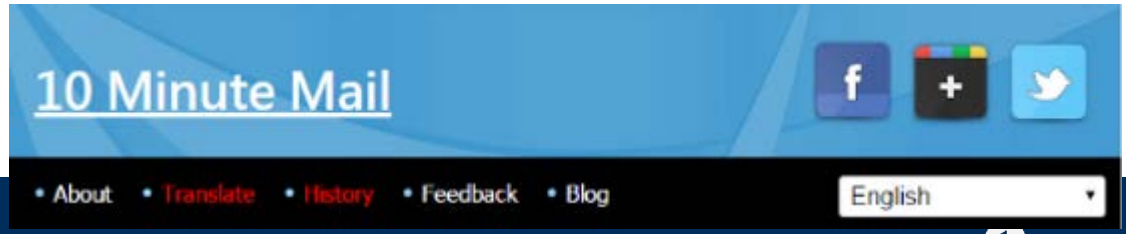
Make all others accountable too.

NEVER EXPECT PRIVACY/SECURITY FROM FREE SOCIAL MEDIA, SEARCH OR BROWSING SERVICES

- Apple Differential Privacy Technology knows your browse habits
- Snap Chat - knows your name (even if you don't give it), who you contact and when, the phone you use and its IMEI!
- Google –search, location, voice searches, audio commands, app activity (disable in web and app activity in activity controls)
  - jgvigorito+websitename.com@gmail.com (see who sells your email)
- Facebook – Allows unknown people to look you up, get your GPS coordinates, your birthday, your hometown (if you post these)
- Use haveibeenpwned.com



- Use 10minutemail.net



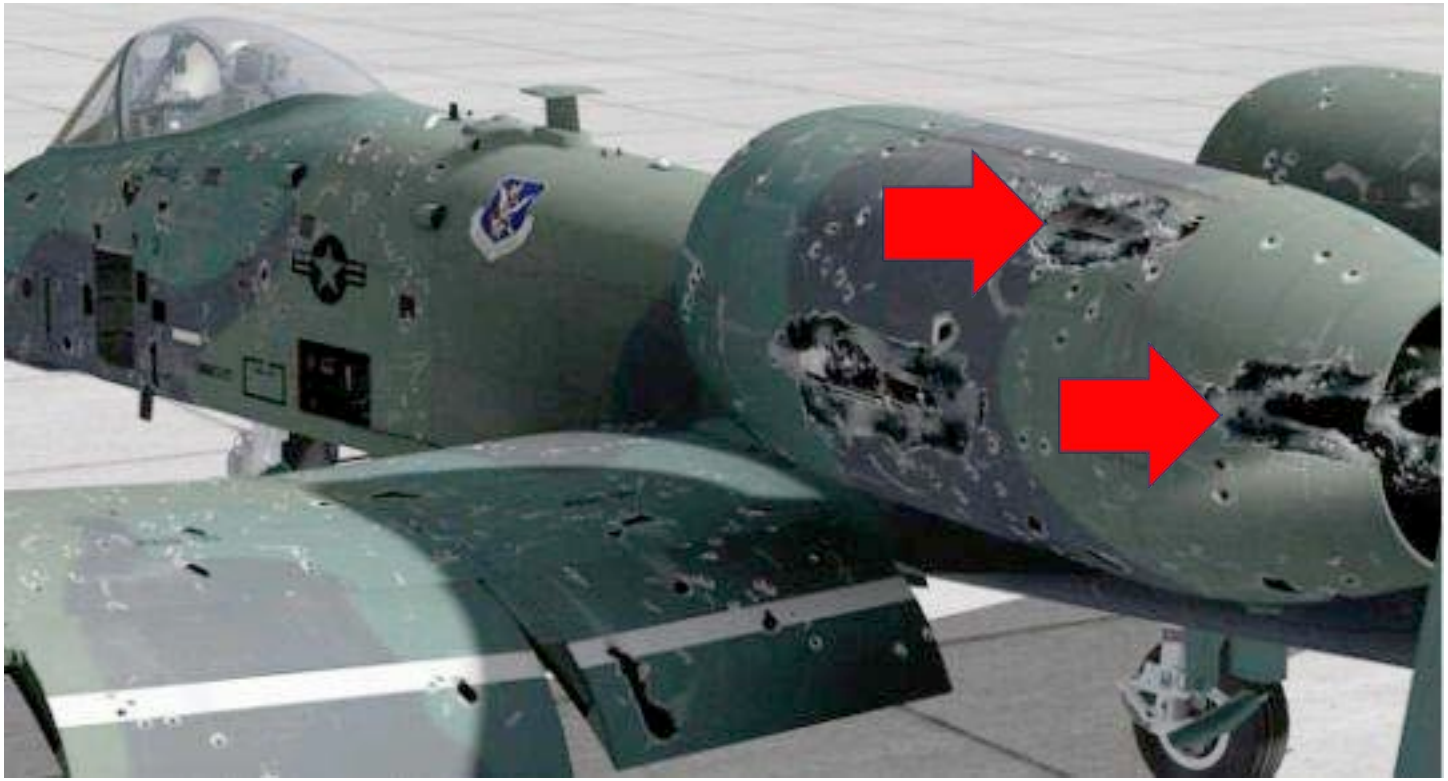
FINAL THOUGHT

Bingham County, Idaho Administrator three weeks ago:

> ***"To prevent ransomware from hitting us again, there will likely be several more firewalls and more training for staff using county computers."***

Statement shows the person does not know the problem, nor the solution. Do not stop educating & learning. Seek assistance.

SO IF YOU THINK YOU ARE HAVING A BAD DAY…



A-10 “Flying Tank”

THANK YOU, WE APPRECIATE YOUR TIME