KnowBe4
Human error. Conquered.

A Master Class on Cybersecurity: Roger Grimes Teaches Data-Driven Defense

Roger A. Grimes
Data-Driven Security Evangelist
rogerg@knowbe4.com

Roger A. Grimes
Data-Driven Defense Evangelist
KnowBe4, Inc.

e: rogerg@knowbe4.com
Twitter: @RogerAGrimes
LinkedIn: https://www.linkedin.com/in/rogeragrimes/

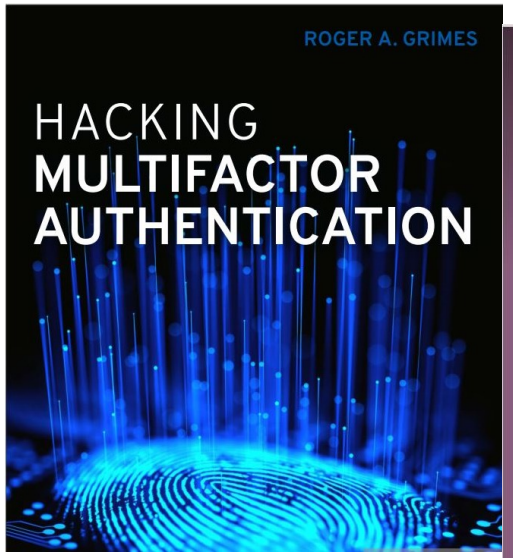
About Roger

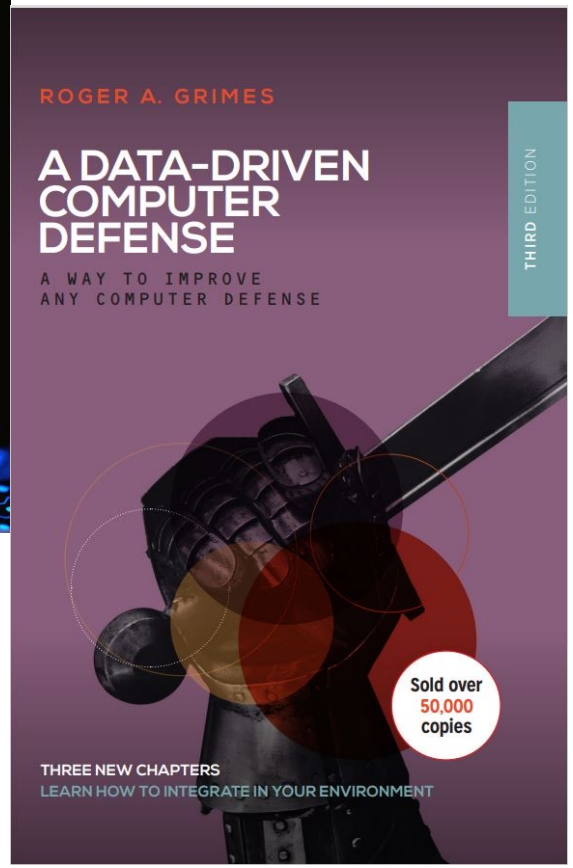
- 34 years plus in computer security, 20 years pen testing
- Expertise in host and network security, IdM, crypto, PKI, APT, honeypot, cloud security
- Consultant to world's largest companies and militaries for decades
- Previous worked for Foundstone, McAfee, Microsoft
- Written 13 books and over 1,300 magazine articles
- *InfoWorld* and *CSO* weekly security columnist 2005 - 2019
- Frequently interviewed by magazines (e.g. Newsweek) and radio shows (e.g. NPR's All Things Considered)

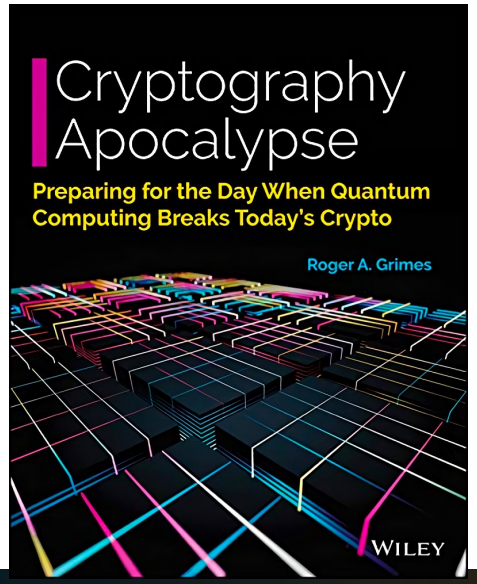
Certification exams passed include:

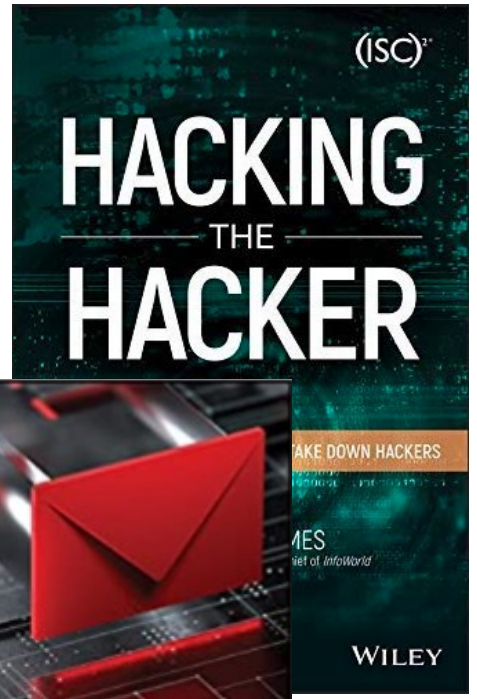
- CPA
- CISSP
- CISM, CISA
- MCSE: Security, MCP, MVP
- CEH, TISCA, Security+, CHFI
- yada, yada

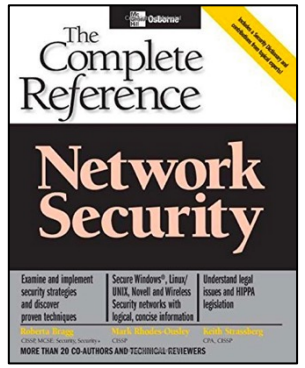
Roger's Books

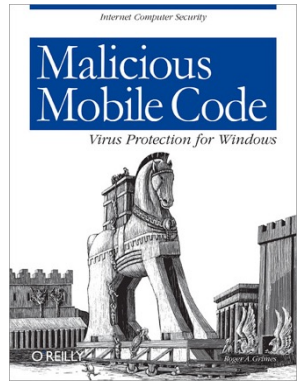


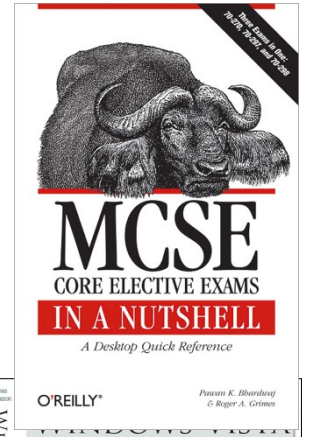


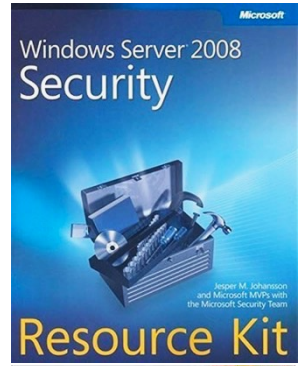


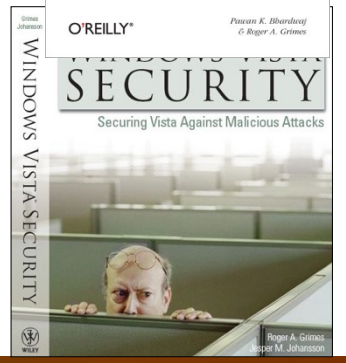


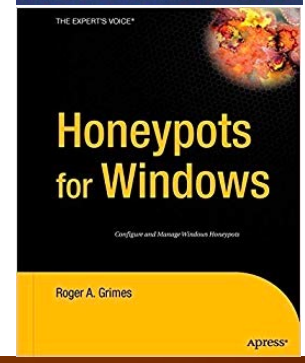












About Us

- The world's largest integrated Security Awareness Training and Simulated Phishing platform
- Based in Tampa Bay, Florida, founded in 2010
- CEO & employees are ex-antivirus, IT Security pros
- We help tens of thousands of organizations manage the ongoing problem of social engineering
- Winner of numerous industry awards

Today's Presentation

- The Biggest Problem With Most Computer Defenses
- How it Got This Way
- How to Fix

Bottom Line Lesson: How to Have a More Efficient, Better, Cost-Effective Defense

Home Crime Allegory

Imagine…

- Houses broken into for decades, usually through a window
- Owner responds by getting stronger doors and more door locks
- Law enforcement, community associations, Consumer Reports, recommend stronger door defenses

This is the way most IT defenders work

If you want to stop break-ins you need to close the holes thieves use to break-in

Data-Driven Defense Summation

- Fighting the right threats first
  - Putting the right defenses in the right places in the right amounts against the right threats

- Most people and organizations don’t fight the biggest threats with the first and best defenses

Data-Driven Defense Summation

In a nutshell:

- How to better evaluate and mitigate cybersecurity risks
- Oftentimes what you are told to fear isn’t really a big risk

Data-Driven Defense Summation

For example:

- Do RFID credit card shielding products make sense?

https://www.linkedin.com/pulse/all-i-want-christmas-certainly-isnt-rfid-credit-card-sleeve-grimes

Data-Driven Defense Summation

For example:

- When Meltdown and Spectre chip flaws came out, did you need to stop what you were doing and patch them?

- How did they compare to Log4j vulnerability?

Most Companies are Inefficient Defenders

Problem Definition

Most Defenders:

- Don’t understand their threats and risks as well as they think they do
- Don’t ask the right questions
- Don’t use their own data to drive solutions
- Don’t put in the right defenses in the right places in the right amounts against the right things
- Poor communication at all levels
- Spend too many resources on the wrong things and end up with the wrong results

Misalignments and inefficiencies abound

Examples of Inefficiencies

Problem Definition

- No one can name the #1 computer security problem with a high degree of accuracy or confidence
- Too many projects, too many top priorities
  - Many times none of them address the top risk(s)
- Unranked or mis-ranked: defenses, controls, training, every list
- Strategic controls don’t map to the tactical things would have the most risk impact

How did it get this way?...After all, nobody wants to defend inefficiently

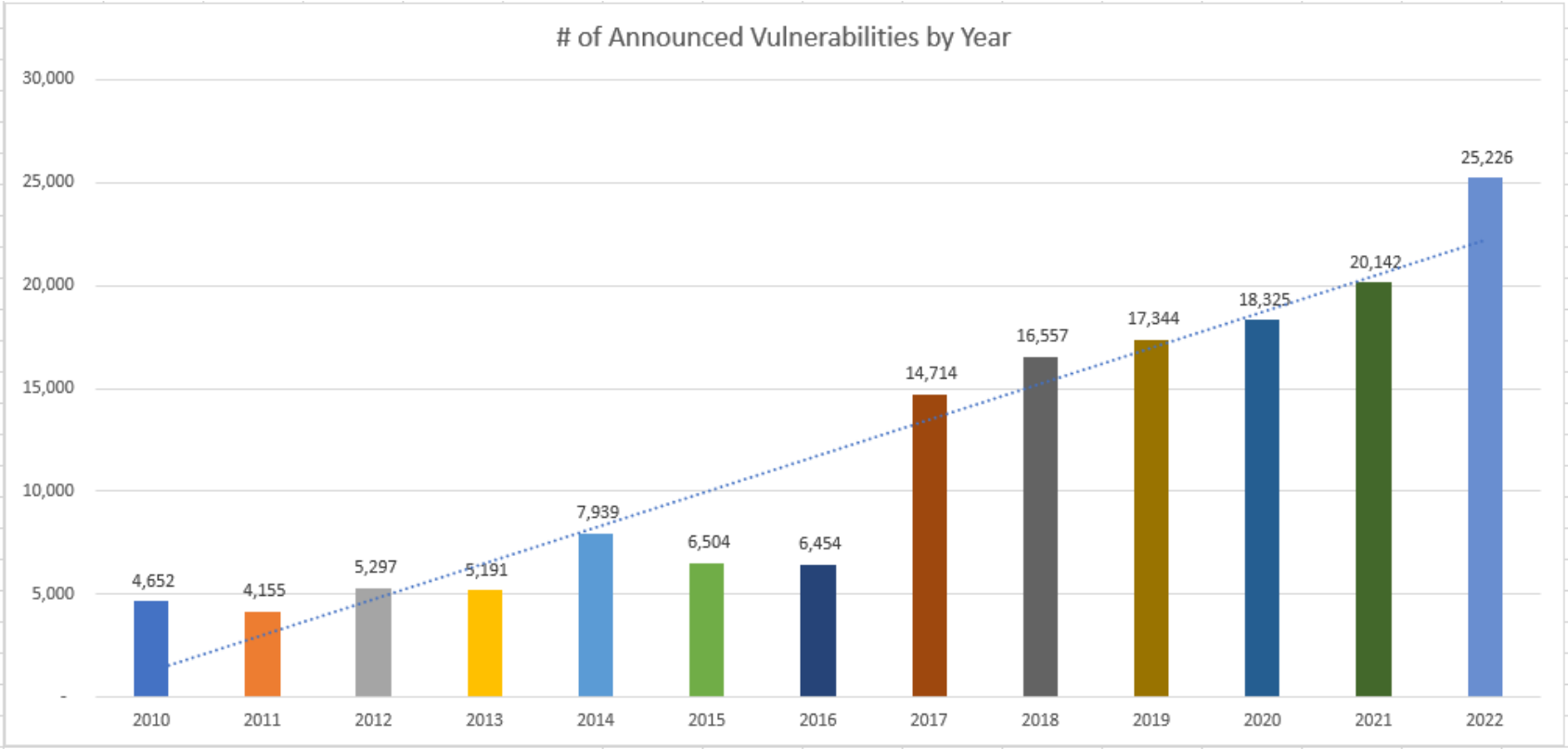
How Did It Get This Way?

Problem – Overwhelming Number of Vulnerabilities

# of Vulnerabilities

- Avg: 4K-25K+ new threats/year
- 11-69/day, day after day

Year	# of vulns
2010	4,652
2011	4,155
2012	5,297
2013	5,191
2014	7,939
2015	6,504
2016	6,454
2017	14,714
2018	16,557
2019	17,344
2020	18,325
2021	20,142
2022	25,226



Source: https://www.cvedetails.com/browse-by-date.php

And this is just (known public) vulnerabilities, doesn't include hackers and a hundred million malware programs

Problem – We Are Taught Wrong and Teach Wrong

Problem Definition –

How Did It Get This Way?

- Nearly every cybersecurity guide and recommendation guide tells you to focus on the wrong things
- Cybersecurity guides often don’t tell you to focus on the number one thing that would best fight hacking

Problem – We Are Taught Wrong and Teach Wrong

Problem Definition –

How Did It Get This Way?

Example – PCI-DSS

https://www.pcisecuritystandards.org/document_library

- Version 4.0 is 356-pages long, 249 controls
- First recommendation is about firewalls which really don't work well to prevent today's attacks
- Requires 38 controls over 21 pages

Problem – We Are Taught Wrong and Teach Wrong

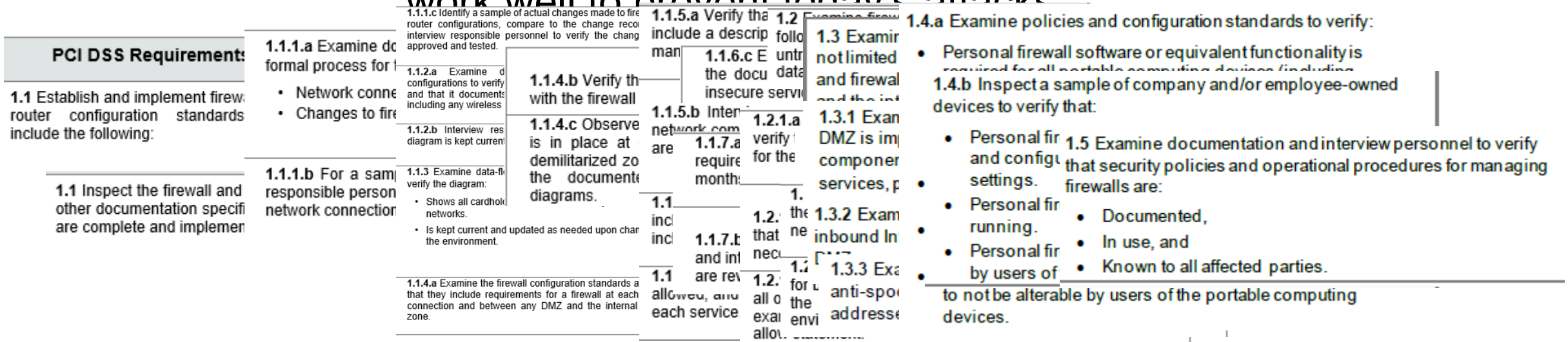
Problem Definition –

How Did It Get This Way?

Example – PCI-DSS

https://www.pcisecuritystandards.org/document_library

- Version 4.0 is 356-pages long, 249 controls
- First recommendation is about firewalls which really don't work well to prevent today's attacks



Problem – We Are Taught Wrong and Teach Wrong

Problem Definition –

How Did It Get This Way?

Example – PCI-DSS

https://www.pcisecuritystandards.org/document_library

- Security awareness training
- Twelfth recommendation, 5 controls, 4 pages
- Training only required once a year

Requirements and Testing Procedures	
12.6 Security awareness education is an ongoing activity.	
Defined Approach Requirements	**Defined Approach Testing Procedures**
12.6.1 A formal security awareness program is implemented to make all personnel aware of the entity's information security policy and procedures, and their role in protecting the cardholder data.	**12.6.1** Examine the security awareness program to verify it provides awareness to all personnel about the entity's information security policy and procedures, and personnel's role in protecting the cardholder data.

Defined Approach Requirements	Defined Approach Testing Procedures
12.6.3 Personnel receive security awareness training as follows: • Upon hire and at least once every 12 months. • Multiple methods of communication are used. • Personnel acknowledge at least once every 12 months that they have read and understood the information security policy and procedures.	**12.6.3.a** Examine security awareness program records to verify that personnel attend security awareness training upon hire and at least once every 12 months. **12.6.3.b** Examine security awareness program materials to verify the program includes multiple methods of communicating awareness and educating personnel. **12.6.3.c** Interview personnel to verify they have completed awareness training and are aware of their role in protecting cardholder data. **12.6.3.d** Examine security awareness program materials and personnel acknowledgments to verify that personnel acknowledge at least once every 12 months that they have read and understand the information security policy and procedures.
Customized Approach Objective	
Personnel remain knowledgeable about the threat landscape, their responsibility for the operation of relevant security controls, and are able to access assistance and guidance when required.	

Problem – We Are Taught Wrong and Teach Wrong

Problem Definition –

How Did It Get This Way?

Example – FBI Hive Ransomware Warning (8/26/21)

https://www.documentcloud.org/documents/21049431-fbi-flash-hive-ransomware-iocs

Indicators of Compromise Associated with Hive Ransomware

Summary

Hive ransomware, which was first observed in June 2021 and likely operates as an affiliate-based ransomware, employs a wide variety of tactics, techniques, and procedures (TTPs), creating significant challenges for defense and mitigation. Hive ransomware uses multiple mechanisms to compromise business networks, including phishing emails with malicious attachments to gain access and Remote Desktop Protocol (RDP) to move laterally once on the network.

Problem – We Are Taught Wrong and Teach Wrong

Problem Definition –

How Did It Get This Way?

Example – FBI Hive Ransomware Warning

https://www.documentcloud.org/documents/21049431-fbi-flash-hive-ransomware-iocs

Recommended Mitigations

- Back-up critical data offline.
- Ensure copies of critical data are in the cloud or on an external hard drive or storage device.
- Secure your back-ups and ensure data is not accessible for modification or deletion from the system where the data resides.
- Use two-factor authentication with strong passwords, including for remote access services.
- Monitor cyber threat reporting regarding the publication of compromised VPN login credentials and change passwords/settings if applicable.
- Keep computers, devices, and applications patched and up-to-date.
- Install and regularly update anti-virus or anti-malware software on all hosts.

- 8 recommendations, none address educating people about social engineering

Problem – Competition for Resources

Problem Definition –

How Did It Get This Way?

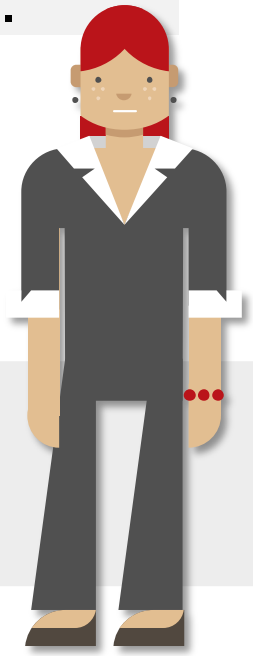
- Avalanche of New Threats
- Media- and Vendor-Driven Narratives
- Compliance Always Wins
- Too Many Projects
- Higher Priority Pet Projects/Politics
- Slower Budgeting Cycles
- Inefficient IT Organization

Problem – Humans are Poor at Risk Evaluation

Evolution: Humans are not great at ranking risks, even when the metrics are known.

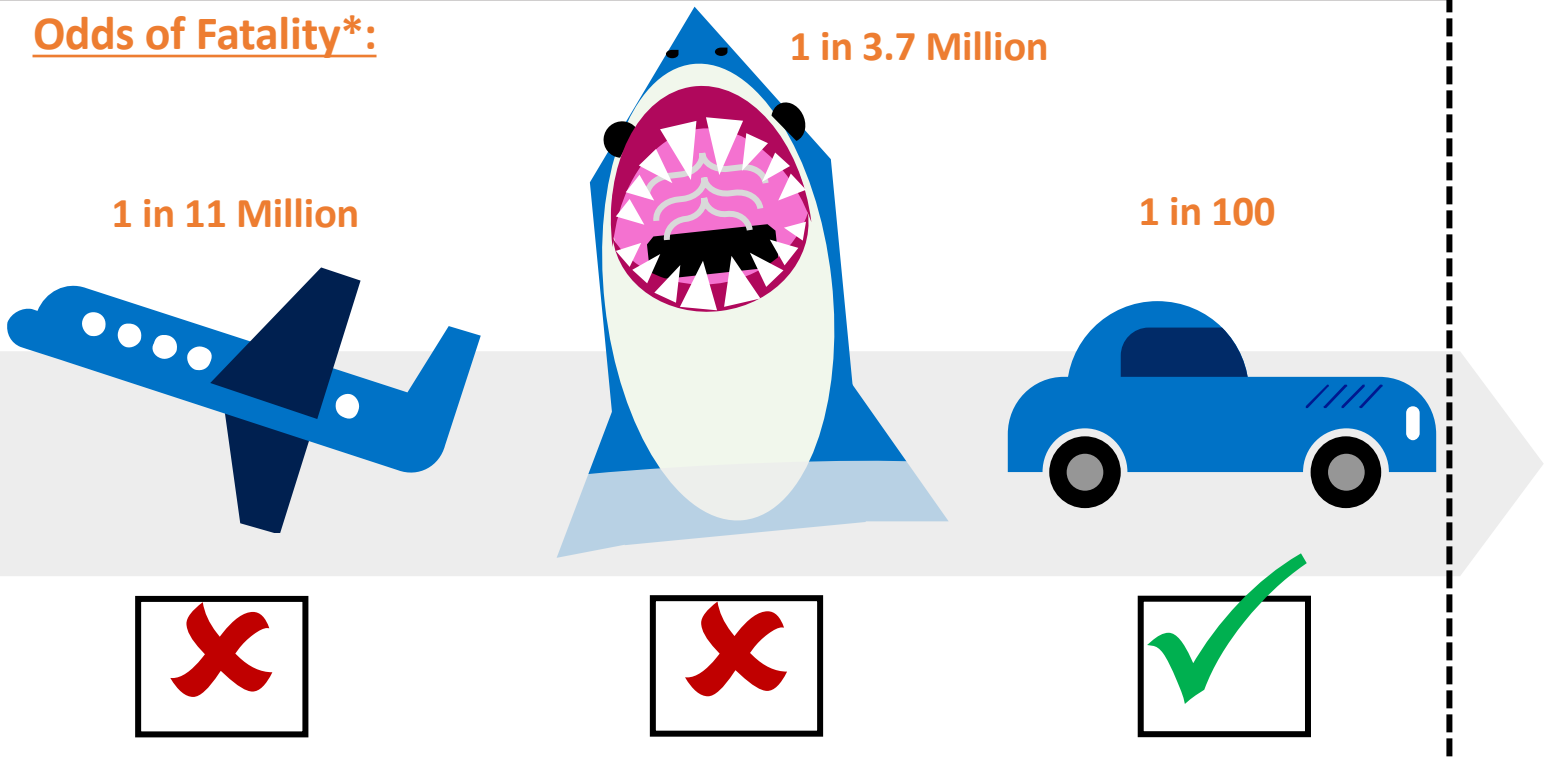
Problem Definition –

How Did It Get This Way?



Example: Most humans are more afraid of **airplane crashes** and **shark attacks** than the car rides to the locations where those events could possibly take place even though the **car ride** is tens of thousands of times more risky

Odds of Fatality*:



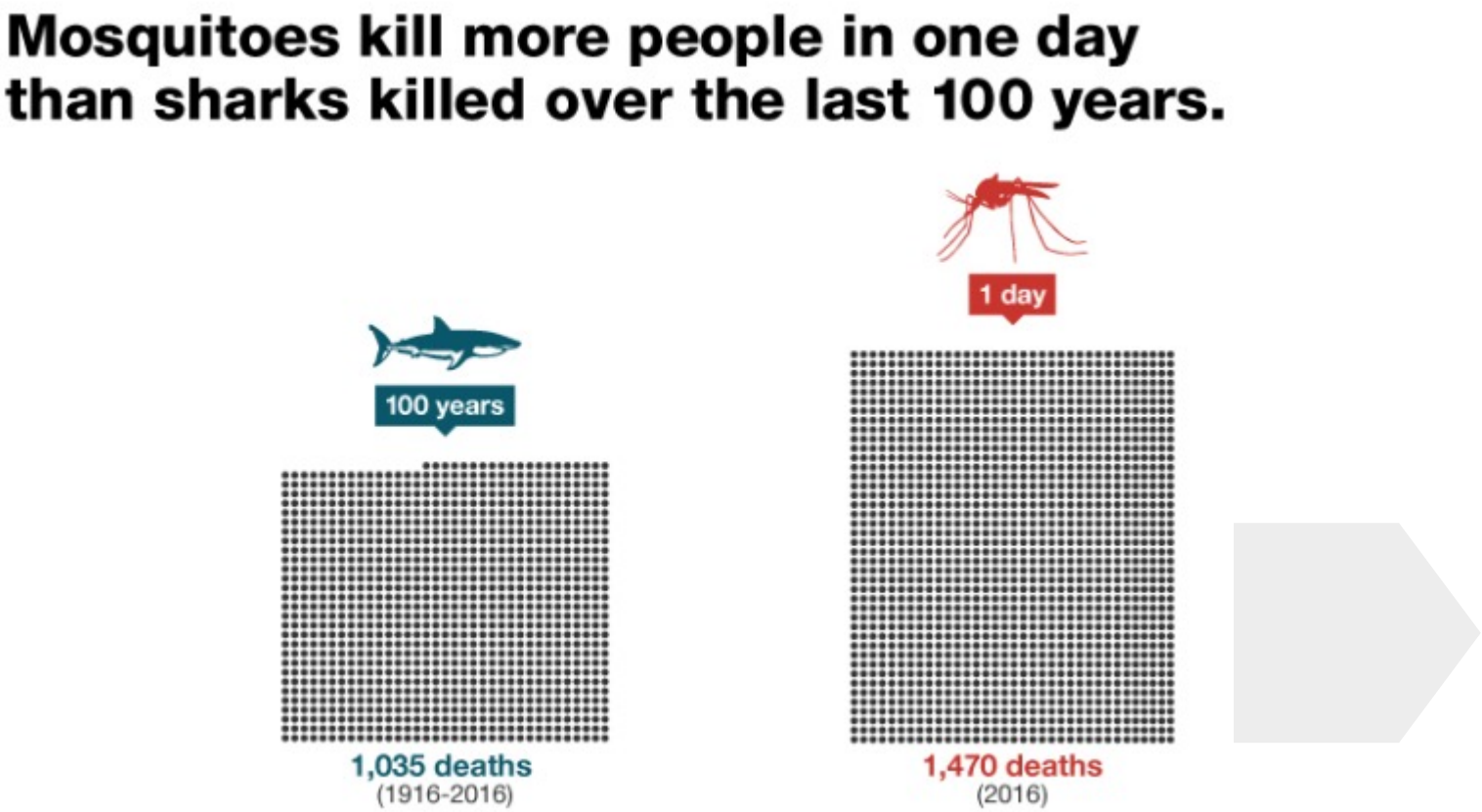
*sources: Clarke, Ropeik, National Geographic

Problem – Humans are Poor at Risk Evaluation

Evolution: Humans are not great at ranking risks, even when the metrics are known.

Problem Definition –

How Did It Get This Way?

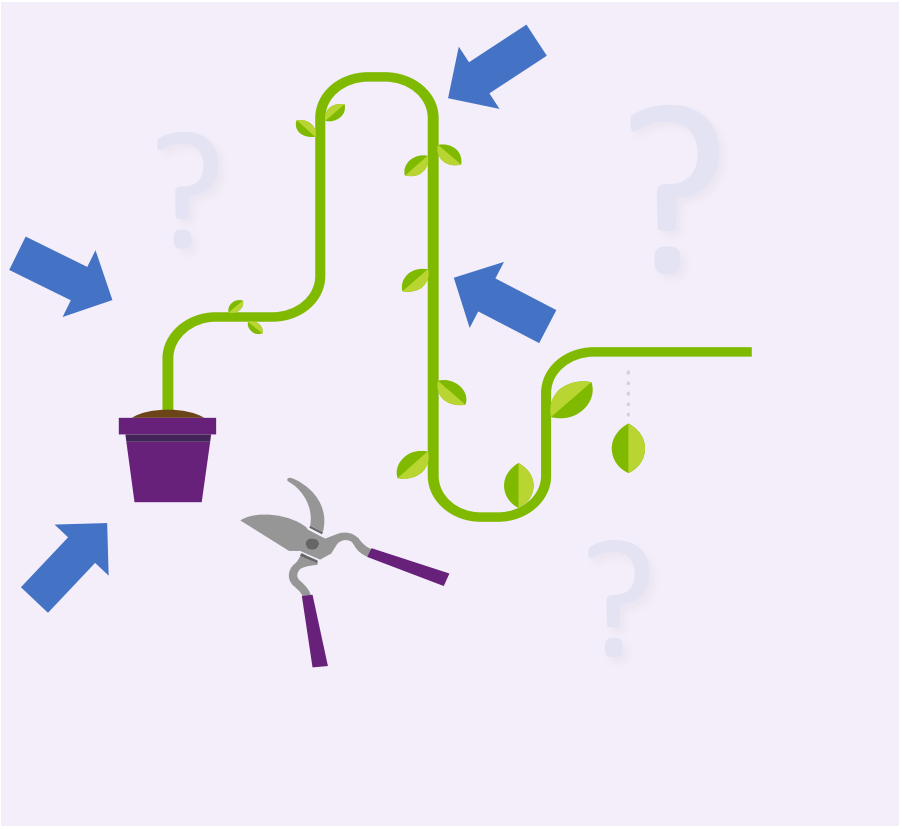


Problem – Not Enough Focus on Initial Access Methods

How attackers/malware break in

What's the number one initial root exploit in your environment?

- Social Engineering
- Programming Bug (patch available or not available)
- Authentication Attack
- Malicious Instructions/Scripting
- Data Malformation
- Human Error/Misconfiguration
- Eavesdropping/MitM
- Side Channel/Information Leak
- Brute Force/Computational
- Network Traffic Malformation
- Insider Attack
- 3rd Party Reliance Issue (supply chain/vendor/partner/etc.)
- Physical Attack



Ask Yourself 3 Key Questions:

1. Can your team correctly answer what is the top initial exploit cause?
2. Is the answer consistent across all stakeholders?
3. Do you have data to back up the right answer?

How Did We Get Here? – Poor Communication

The Security Communication Problem

<u>Even if IT security team could identify top threats:</u>
Lack of good, clear communications from top to bottom

- Training doesn't focus consistently on top threats
- End-users can't identify top threats

- Senior management isn't told the top threats
- Senior management can't provide the right resources and controls in the right places because they haven't been given the right threat prioritization
- Strategic controls often don't include enough tactical details to drive best security solutions

Lack of objective data prevents effective communication of top threats across enterprise

How Did We Get Here? – Lack of Good Data

Lack of useful, objective data prevents effective defense against top threats

The Data Problem

- Too much data
- Not enough useful, meaningful data
- Too much useless “noise”
- Good data sitting under utilized
- Data gaps not being recognized
- People not asking the right questions
- Not enough people asking for data to back up claims

Poor Risk Ranking

Leads to IT Defenders:

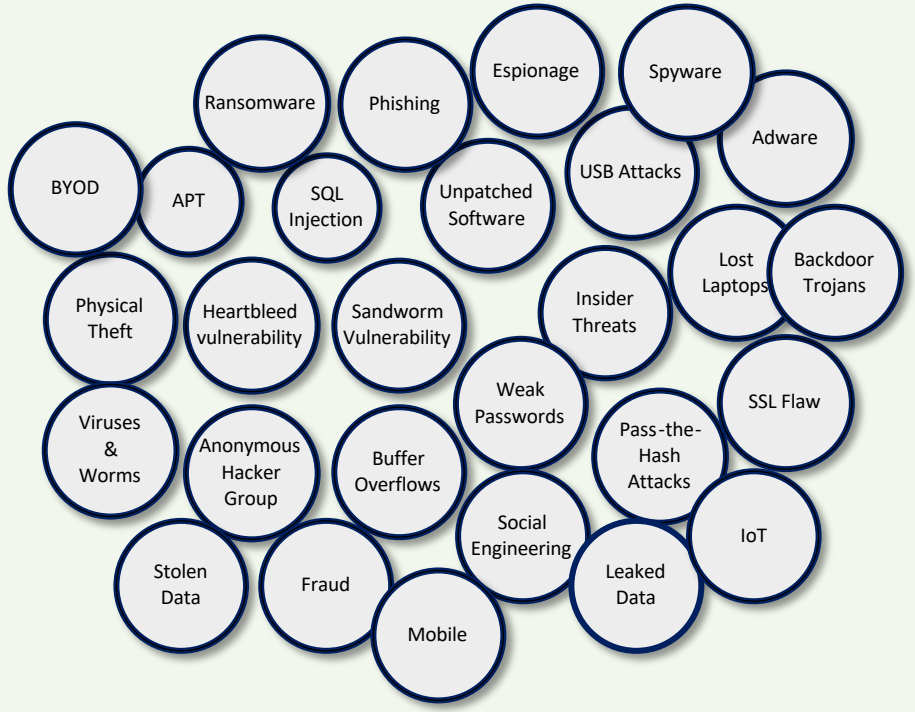
- Not ranking risks correctly relative to each other
- Seeing all risks as more equal than they are
- Focusing on the wrong threats
- Focusing on individual threats instead of more inclusive, broader root cause issues
- Belief that malicious events are impossible to stop or minimize (“assume breach”)

Can lead to a sense of hopelessness by defenders and the people who rely on those defenders

The Traditional Approach to IT Security Risks

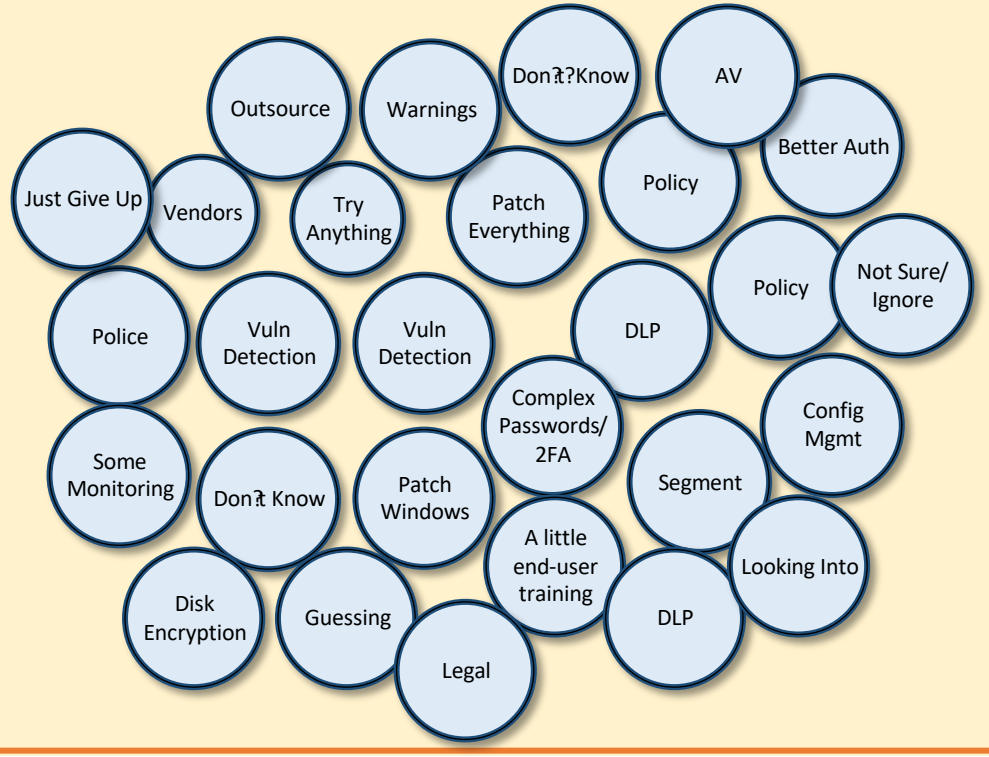
Poor risk analysis leads to mis-ranked, whack-a-mole", defenses

How most defenders see threats



"Like bubbles in a glass of champagne"

How they apply Defenses



"Every defense is treated equally, or applied disproportionate to risk

The Solution

What is a Data-Driven Computer Defense?

What is it?: A methodology that allocates security resources more efficiently and effectively, to mitigate the top computer and network security threats faster and cheaper using risk analytics.

A strategy which uses relevant data and focuses on:

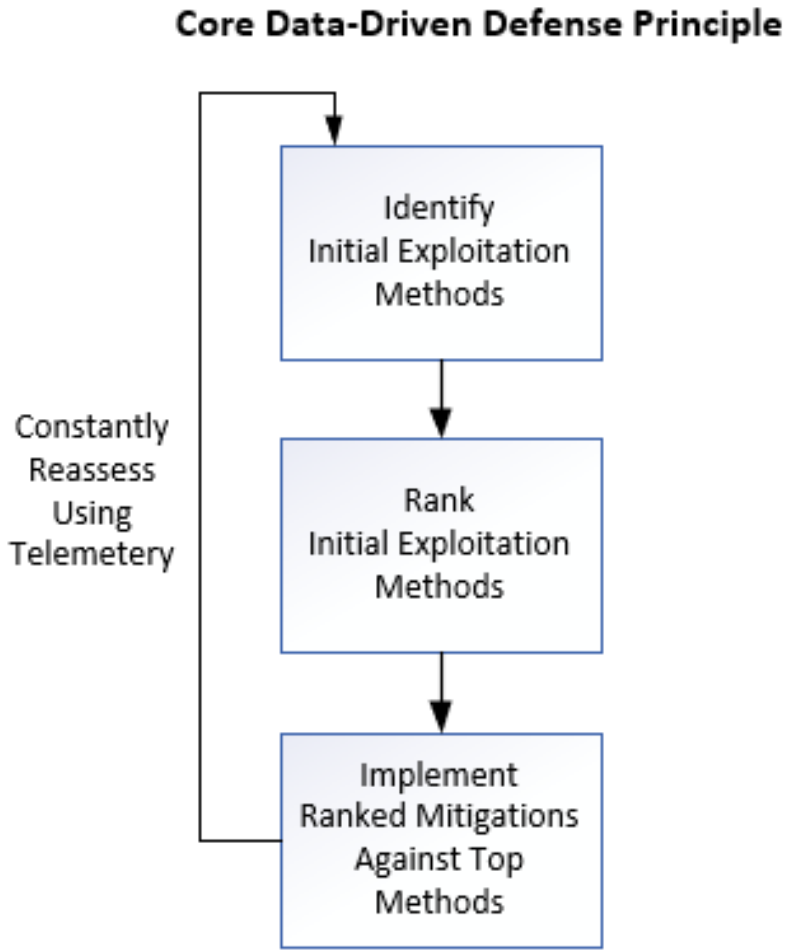
- Better risk ranking the most-likely threats
- Local threat and attack experience
- Root causes of initial breaches
- Asking the right questions
- Getting and using good data
- Selecting the right defenses
- Better communications

First described in Sept. 2015 Microsoft whitepaper: https://bit.ly/32Ytto6

Initial Root Access Exploit Methods

How ALL attackers/malware break in

- Social Engineering
- Programming Bug (patch available or not available)
- Authentication Attack
- Malicious Instructions/Scripting
- Human Error/Misconfiguration
- Eavesdropping/MitM
- Side Channel/Information Leak
- Brute Force/Computational
- Data Malformation
- Network Traffic Malformation
- Insider Attack
- 3rd Party Reliance Issue (supply chain/vendor/partner/etc.)
- Physical Attack



Focus on Initial Root Causes

You should care most about root causes of initial breaches

Ransomware isn't the problem. It's how ransomware got in

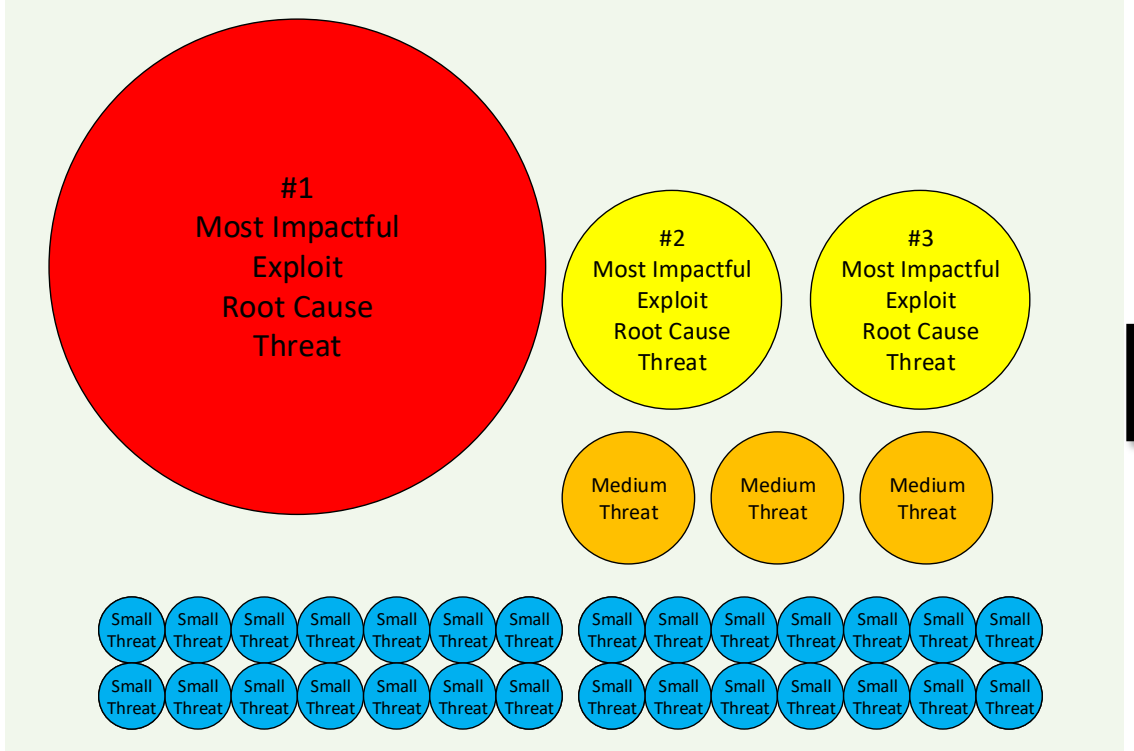
Focusing on individual threats and only what they did after they got in is like worrying about your brakes after your car is stolen

When you've adjusted your thinking, adware is as worrisome as a malicious backdoor remote access Trojan or ransomware

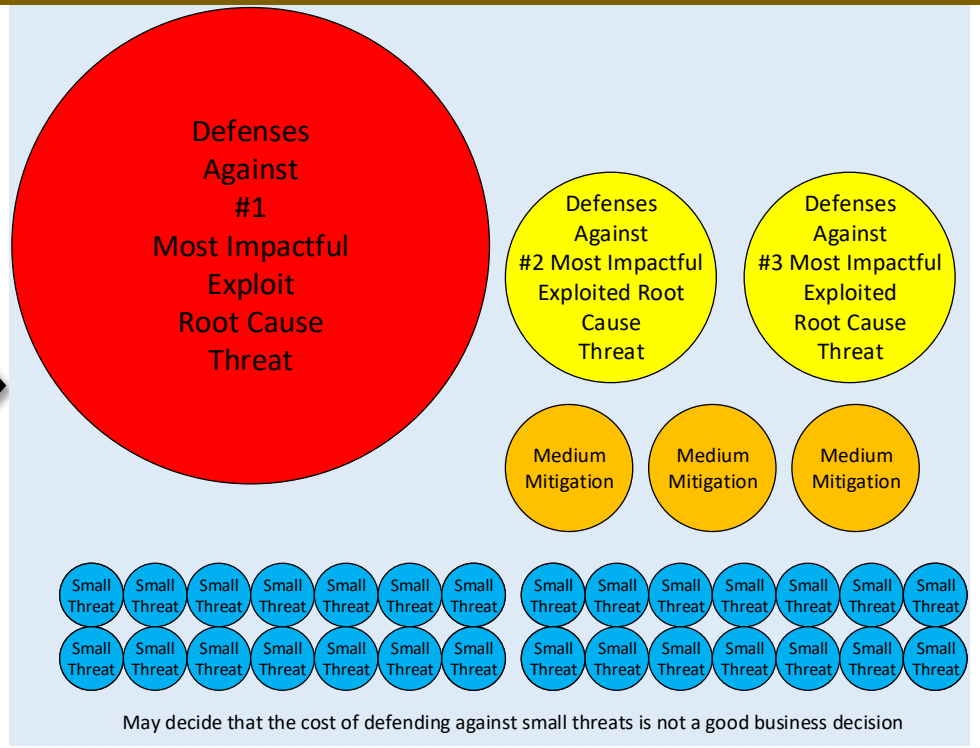
<u>Both took the same effort to get into your environment</u> and is revealing defensive gaps

The Data-Driven Defenders Approach

The Data-Driven Threat Perception



Data-Driven Defense Application



Risk Ranked Threat Perceptions:

- Focuses on root causes
- Local experience and data is highly valued
- Relevance is a big deciding factor

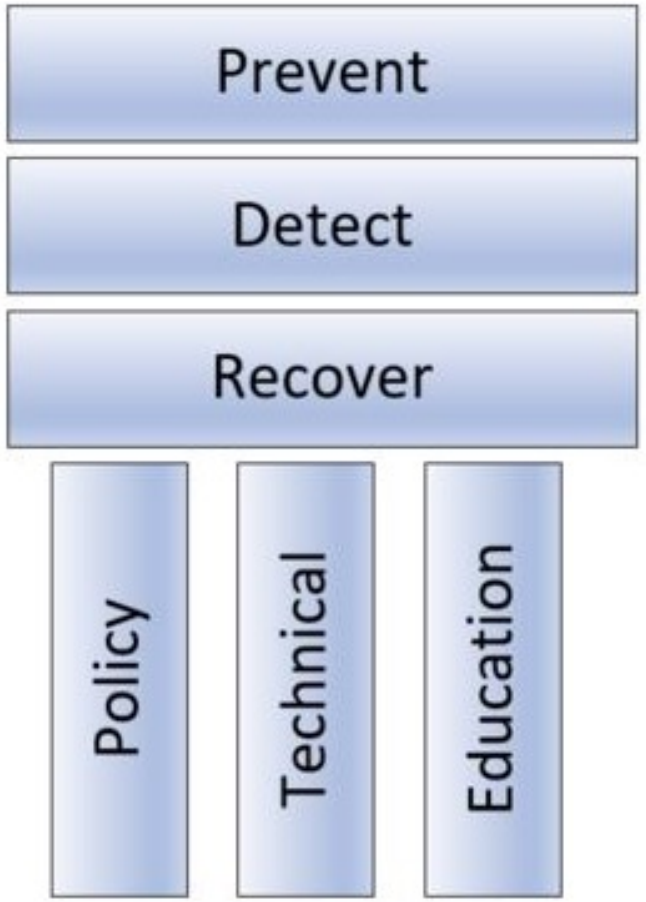
Risk Ranked Defenses:

- Mitigates root causes, not individual threats
- More efficient resource utilization
- Allows clearer cost/benefit considerations

Defending Against Phishing

General Defense Methods

- Policies
- Technical Defenses
  - Anti-Malware Software
  - Anti-Spam/Phishing
  - Content Filtering
- Security Awareness Training

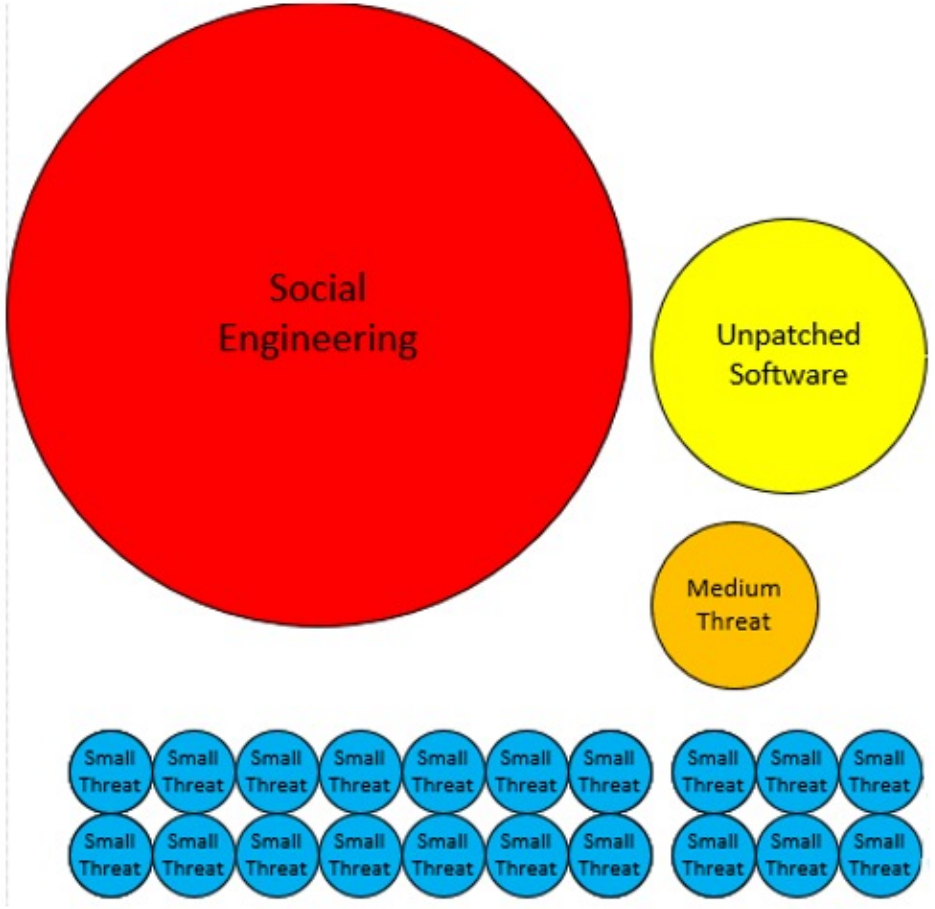


https://blog.knowbe4.com/the-three-pillars-of-the-three-computer-security-pillars

Biggest Initial Breach Root Causes for Most Companies

- Social Engineering
- Unpatched Software

- But don't trust me, measure your own risk



Social engineering is responsible for majority of all malicious data breaches

https://blog.knowbe4.com/70-to-90-of-all-malicious-breaches-are-due-to-social-engineering-and-phishing-attacks

Biggest Initial Breach Root Causes for Most Companies

Meta-Study

- Javvad Malik looked at a 100 cybersecurity reports
- And every report said social engineering was the number one root cause of hacking and malware

Social engineering is responsible for majority of all malicious data breaches

https://info.knowbe4.com/threat-intelligence-to-build-your-data-driven-defense

How Ransomware Attacks

Top Ransomware Root Exploit Causes (in order)

- Social Engineering
- RDP Attacks
- Unpatched Software
- Password Attacks
- Other

Report Name	Social engineering	Unpatched software	Remote server attack	RDP	Password Guessing	Credential Theft	Third Party	USB	Other
Coveware Report	30%	18%	-	45%	-	-	-	-	5%
Statisca	54%	-	-	20%	-	10%	-	-	-
Forbes magazine article	1st	2nd	-	3rd	-	-	-	-	-
Datto's Report	54%	-	-	20%	21%	10%	-	-	-
Hiscox Cyber Readiness	65%	28%	-	-	19%	39%	34%	-	-
Sophos Report	45%	-	21%	9%	-	-	9%	7%	9%
Averages	50%	23%	21%	24%	20%	20%	22%	7%	7%

https://info.knowbe4.com/wp-root-causes-ransomware

Best Defenses

Top Defenses for Most Organizations

- **Mitigate Social Engineering**
  - Policies, Technical Defenses, Education
    - https://info.knowbe4.com/comprehensive-anti-phishing-guide
- **Patch Internet-accessible software**
  - https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- **Use Multifactor Authentication(MFA)/Non-Guessable passwords**
  - Use non-phishable MFA where you can
    - https://www.linkedin.com/pulse/my-list-good-strong-mfa-roger-grimes
  - Use unique, unguessable, different passwords for every website and service
  - Password manager, 12-char fully random or 20-character human-created passphrases
    - https://blog.knowbe4.com/password-policy-e-book
- **Teach Everyone How to Spot Rogue URLs**
  - https://blog.knowbe4.com/top-12-most-common-rogue-url-tricks
  - https://info.knowbe4.com/rogue-urls

Focus on Better (Local) Threat Intelligence

Focus Prioritization:

1. Focus on YOUR **current**, most likely **future**, and **historic** attacks first
2. **New**, most likely to happen, "in-the-wild" and industry targeting
3. **Everything Else**

"The Main Driver is Local Threat Intelligence"

Focus on Top Exploit Methods

Usually 2-3 root cause threats are the vast majority of real risk

Concentrate on, in order of decreasing importance:

- **Exploits Actively <u>Successfully</u> Used Against You**
- **Exploits Likely to Be Used Against <u>Successfully</u> You In the Near Future**
- **Exploits Used Successfully Against You In the Recent Past**

<u>Everything Else</u>

- **Widely Used Current In-the-Wild Exploits**
- **Patch Announced, Likely to be Exploited**
- **Public Exploits Announced**

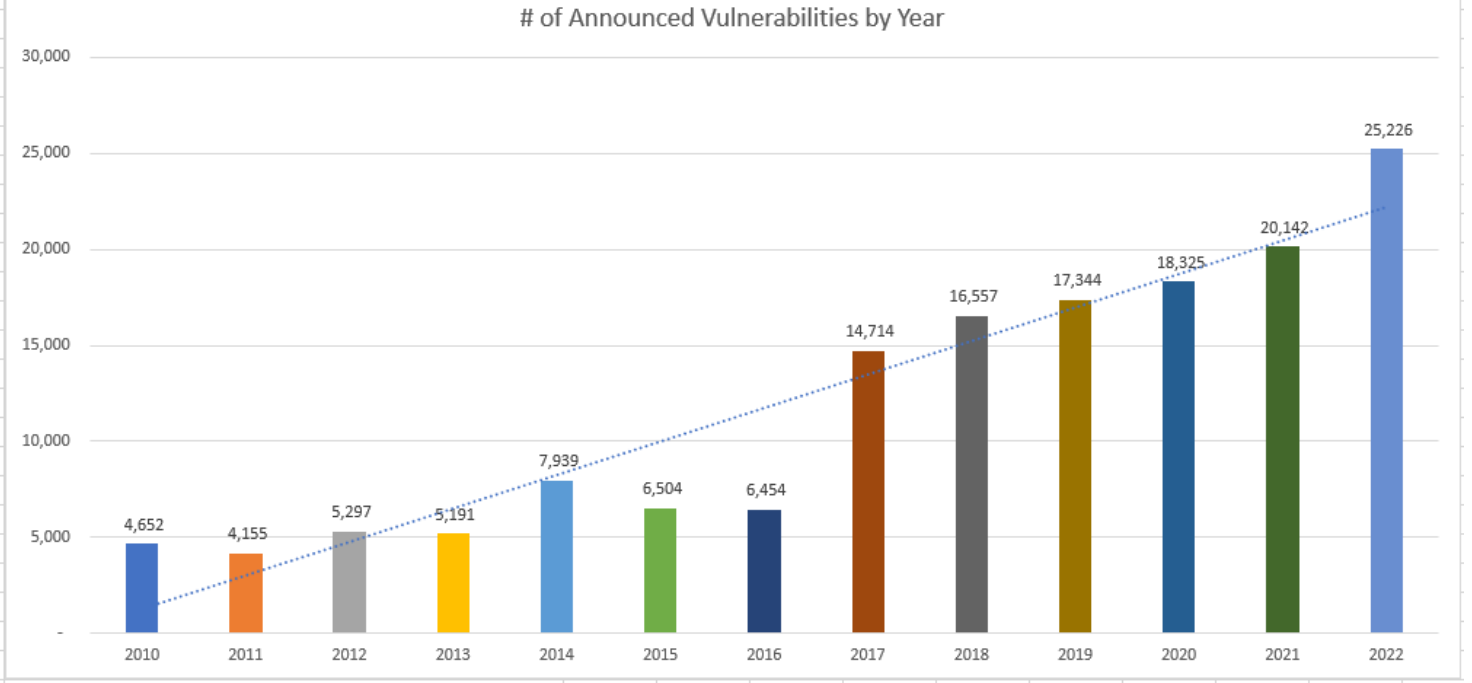
What are your top threats?

What to Patch First and Best?

Problem Summary – Patching Compliance Example

- No one can patch everything perfectly all at once
- There were 25,226 publicly announced vulnerabilities last year

Year	# of vulns
2010	4,652
2011	4,155
2012	5,297
2013	5,191
2014	7,939
2015	6,504
2016	6,454
2017	14,714
2018	16,557
2019	17,344
2020	18,325
2021	20,142
2022	25,226



Source: https://www.cvedetails.com/browse-by-date.php

What to Patch First and Best?

Problem Summary – Patching Compliance Example

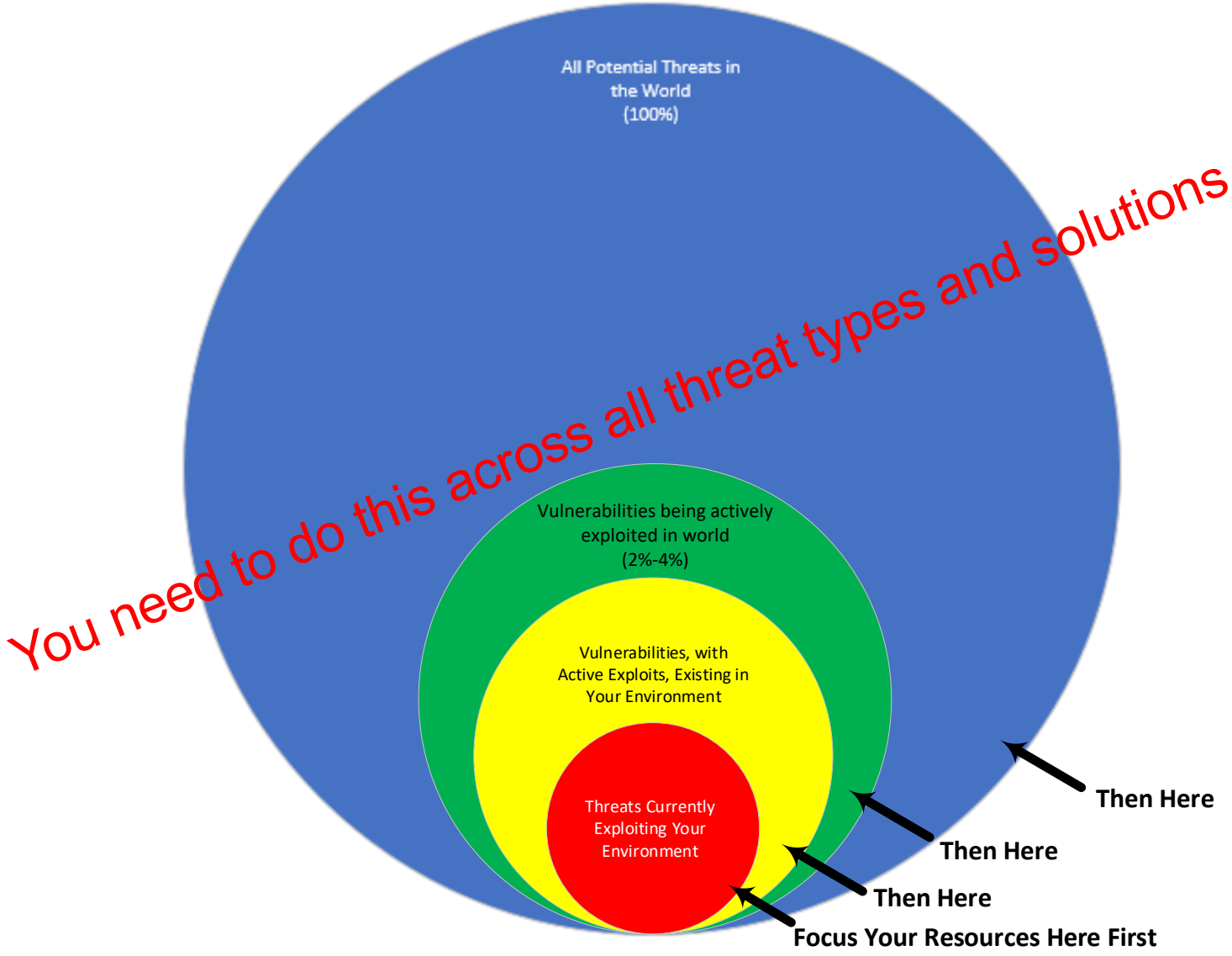
- Only 2% to 4% were used against any company
- Vulnerabilities aren't truly "critical" risks until there is known exploit code and it is being used in the wild

KNOWN EXPLOITED VULNERABILITIES CATALOG

CVE	Vendor/Project	Product	Vulnerability Name	Date Added to Catalog	Short Description	Action	Due Date	Notes
CVE-2021-44077	Zoho	ManageEngine ServiceDesk Plus (SDP) / SupportCenter Plus	Zoho ManageEngine ServiceDesk Plus Remote Code Execution	December 1, 2021	Zoho ManageEngine ServiceDesk Plus before 11306, ServiceDesk Plus MSP before 10530, and SupportCenter Plus before 11014 are vulnerable to unauthenticated remote code execution	Apply updates per vendor instructions.	December 15, 2021	
CVE-2018-14847	MikroTik	RouterOS	MikroTik Router OS Directory Traversal Vulnerability	December 1, 2021	MikroTik RouterOS through 6.42 allows unauthenticated remote attackers to read arbitrary files and remote authenticated attackers to write arbitrary files due to a directory traversal vulnerability in the WinBox interface.	Apply updates per vendor instructions.	June 1, 2022	
CVE-2021-40438	Apache	Apache	Apache HTTP Server-Side Request Forgery (SSRF)	December 1, 2021	A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.	Apply updates per vendor instructions.	December 15, 2021	

- https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- https://www.linkedin.com/pulse/cisa-says-fix-right-stuff-now-roger-grimes/

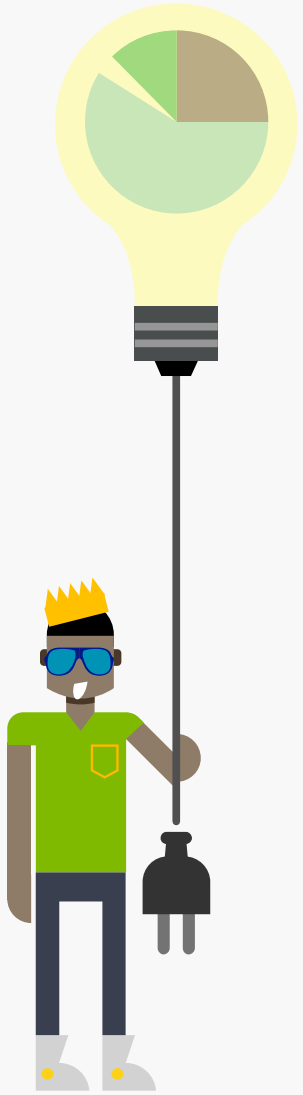
What to Patch First and Best?



Some Other Data-Driven Defense Examples

- Conficker
- Focused Education
- Group Policy Decisions
- Focused Patching
- Social Engineering Training
- Mean-Time-to-Detect
- Driving Red Teams
- Risk Analysis
- Driving Vulnerability Ratings and Remediation Work
- Inventory Analysis

Your Examples of a Data-Driven Defense



Your Examples Can Be:

- Live a career that better focuses on recognizing the right risks
- Makes sure everyone understands biggest attacks and threats
- Make sure your defenses are right-aligned against your biggest threats
- No un-ranked IT security lists or tasks anymore!
- Collect the right data (ex. mean time to detect, AppLocker)
- Social engineering training – more than 30 minutes a year

Questions?

Roger A. Grimes– Data-Driven Defense Evangelist, KnowBe4
rogerg@knowbe4.com
Twitter: @rogeragrimes
https://www.linkedin.com/in/rogeragrimes/