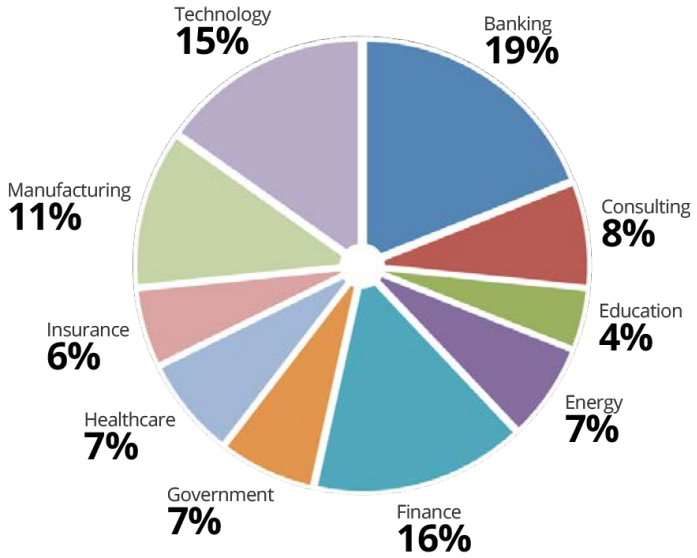
KnowBe4
Human error. Conquered.

Never Assume Breach:
Building a Data-Driven Defense Strategy to Secure Your Organization's Most Valuable Assets

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

KnowBe4, Inc.

- The world's most popular integrated Security Awareness Training and Simulated Phishing platform
- Based in Tampa Bay, Florida, founded in 2010
- CEO & employees are ex-antivirus, IT Security pros
- 200% growth year over year
- We help tens of thousands of organizations manage the problem of social engineering



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

Twitter: @rogeragrimes
LinkedIn: www.linkedin.com/in/rogeragrimes

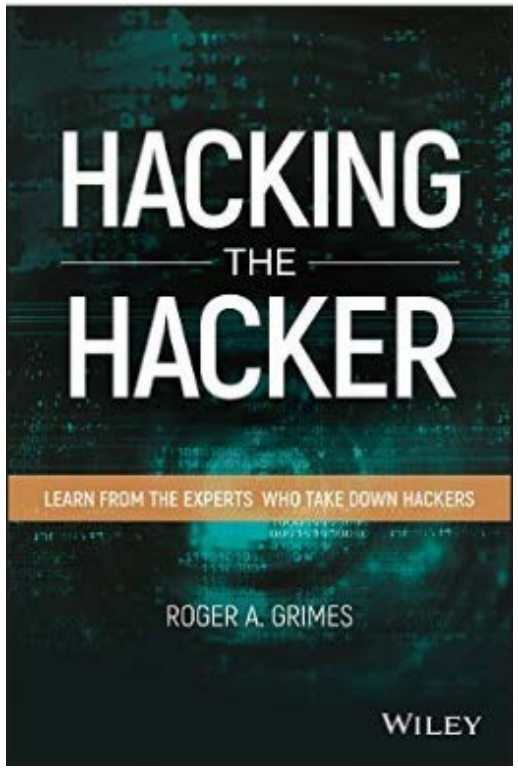
About Roger

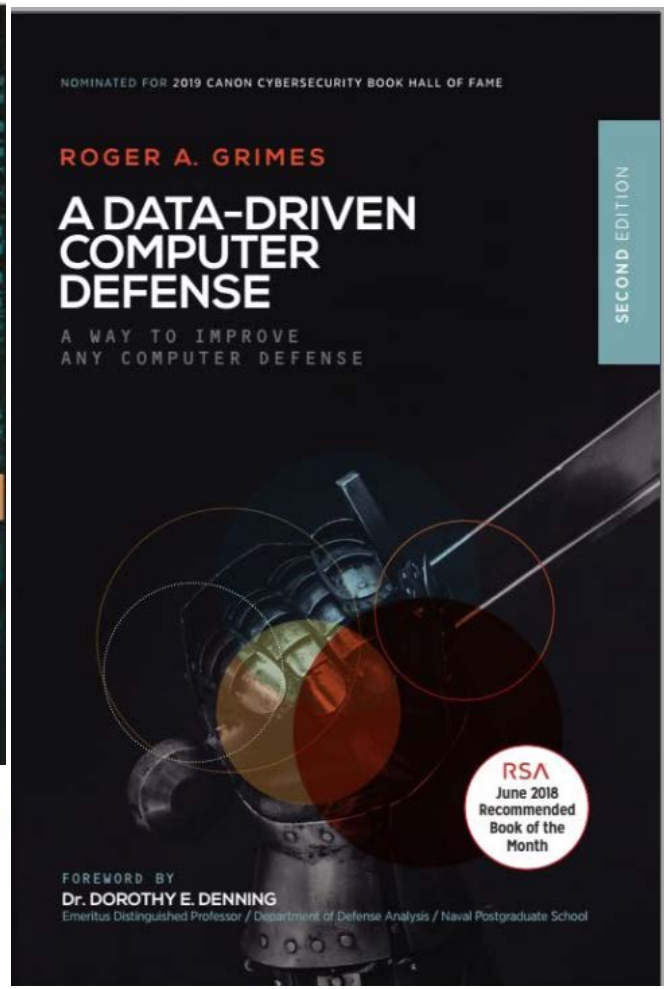
- 30 years plus in computer security
- Expertise in host and network security, IdM, crypto, PKI, APT, honeypot, cloud security
- Consultant to world's largest companies and militaries for decades
- Previous worked for Foundstone, McAfee, Microsoft
- Written 11 books and over 1,000 magazine articles
- *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)

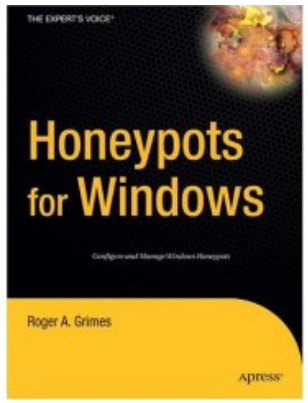
Certification exams passed include:

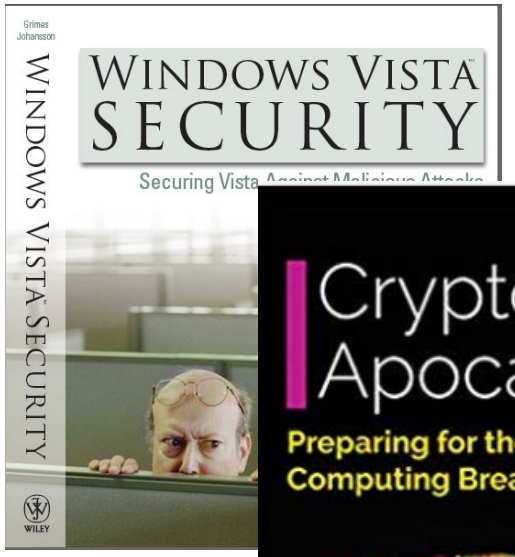
- CPA
- CISSP
- CISM, CISA
- MCSE: Security, MCP, MVP
- CEH, TISCA, Security+, CHFI
- yada, yada

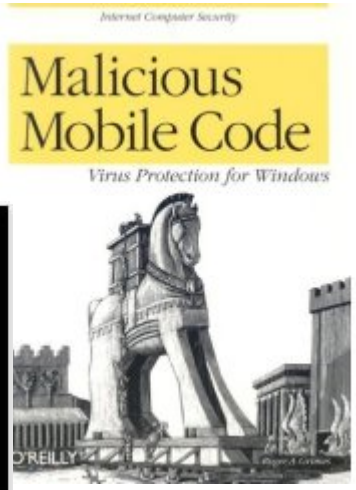
Roger's Books

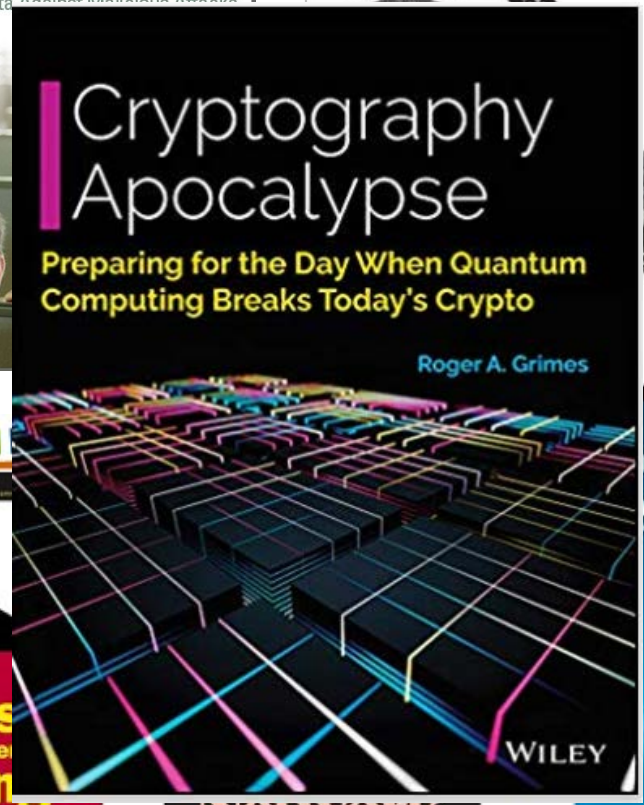


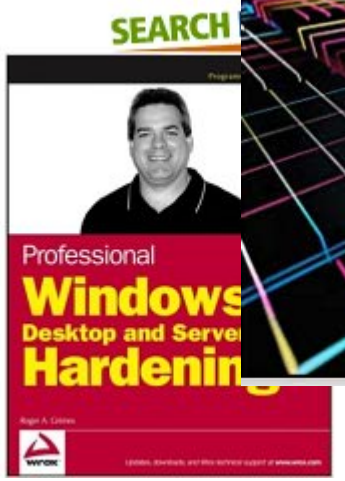


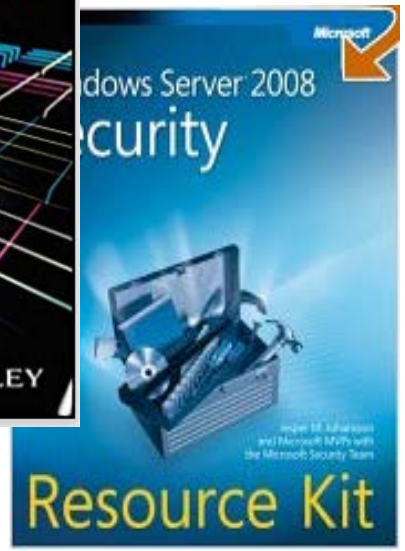












https://www.amazon.com/Data-Driven-Computer-Defense-Way-Improve/dp/1092500847/

Today's Presentation

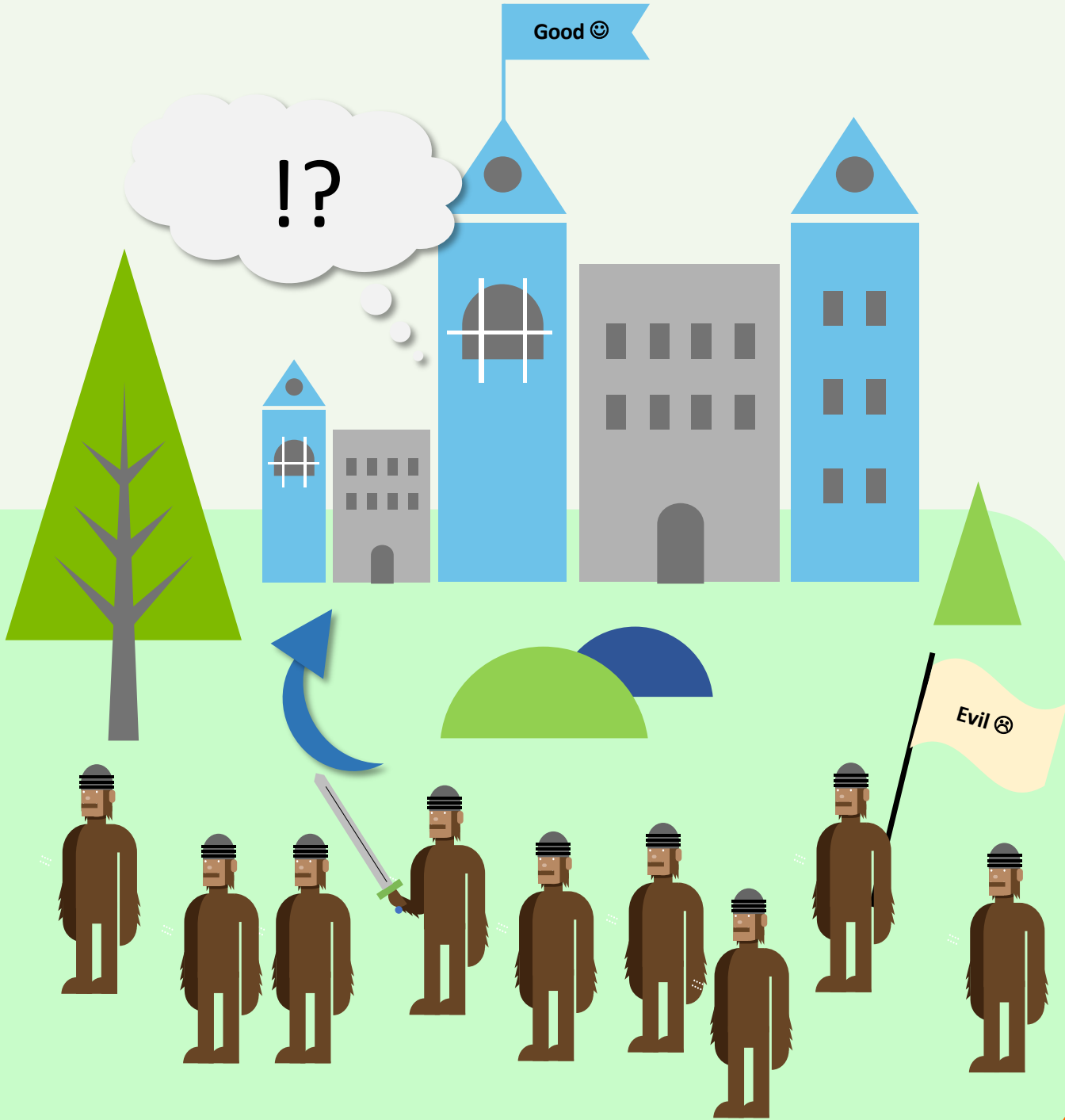
- How to Have a More Efficient, Better, Cost-Effective Defense
- The Biggest Problem With Most Computer Defenses
- How it Got This Way
- How to Fix

The Epic of IT Defenders

Imagine an Army…

- Two sides – good and evil – engaged in a decades long battle
- Evil side is having great success on left flank of battle
- Good side responds by building up right flank and even building up in the center, and wonders why their defense is not working

This is the way most IT defenders work



Data-Driven Defense Summation

- Fighting the right threats
  - Putting the right defenses in the right places in the right amounts against the right threats
- Asking the right questions to make a better defense
- There is a huge gulf between what you are being told are your biggest threats and what your biggest threats really are

Data-Driven Defense Summation

In a nutshell

- How to better evaluate and mitigate cybersecurity risks

For example:

- Do RFID credit card shielding products make sense?
- When Meltdown and Spectre chip flaws came out, did you need to stop what you were doing and patch them?

Definition

Common Understanding – Threats and Risks

- We are worried most about **successful** threats that make it past your current defenses, if even only for a minute before they are detected and removed
- Because it is a symptom of security gaps

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 and 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
- Good patching of low risk apps and poor patching of high risk apps
- 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 Numbers

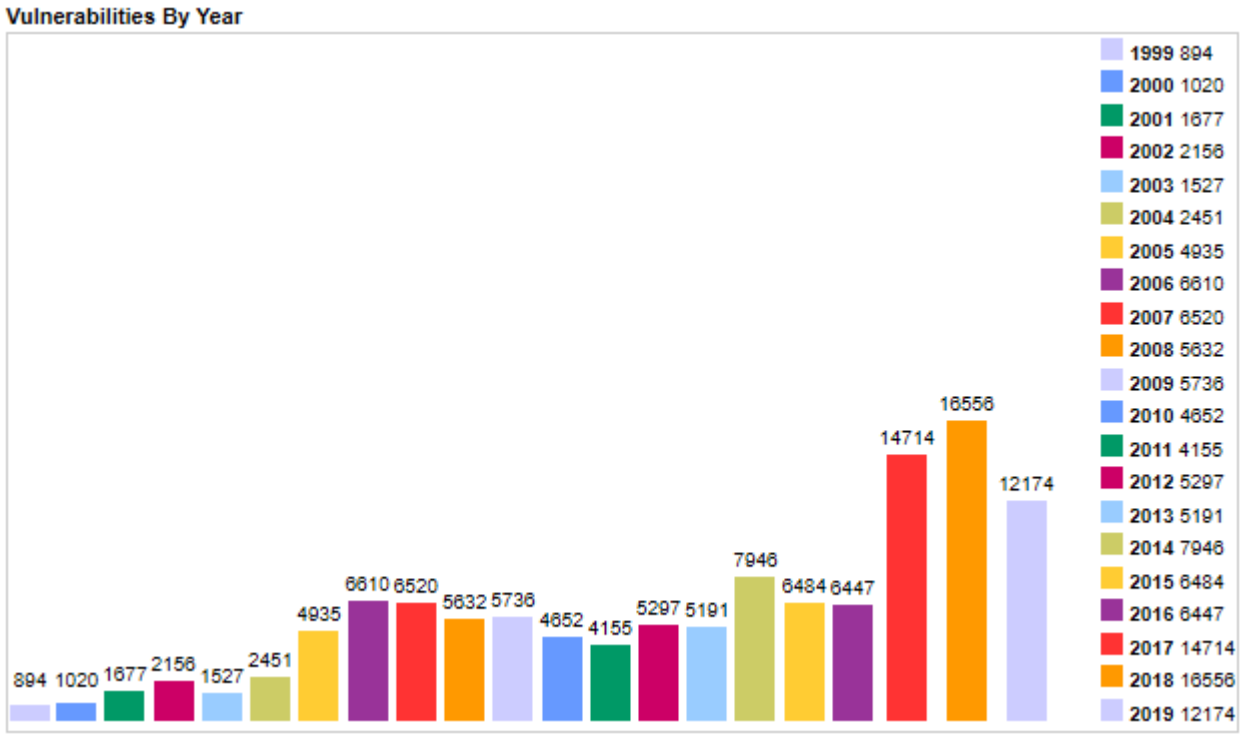
Problem Definition –

How Did It Get This Way?

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

Sheer Number of Threats

- Avg: 5K-16K+ new threats/year
- 13-45/day, day after day



Problem – Too Many Top Priorities

Problem Definition –

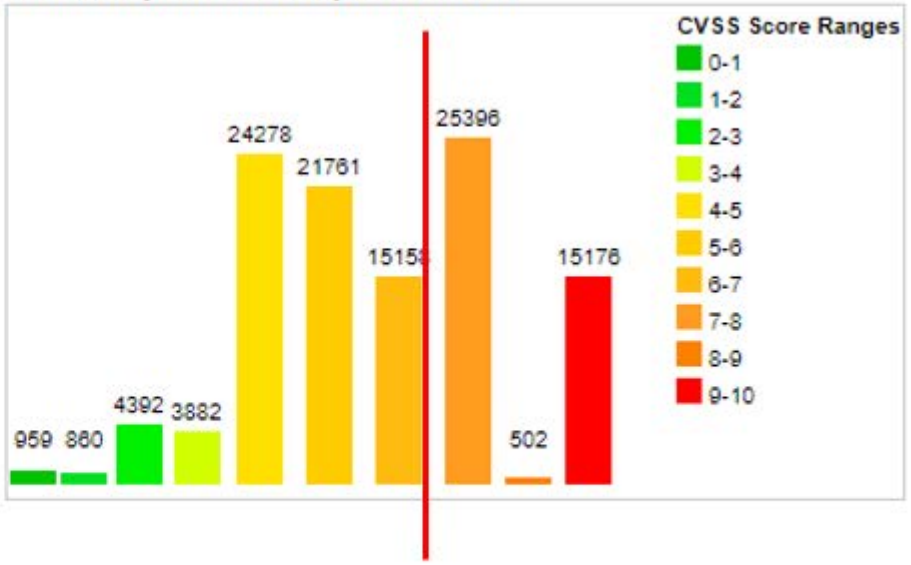
How Did It Get This Way?

- 1/4th to 1/3rd of all vulnerabilities are ranked with the highest criticality

That means thousands of high risk vulnerabilities a year

Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	959	0.90
1-2	860	0.80
2-3	4392	3.90
3-4	3882	3.50
4-5	24278	21.60
5-6	21761	19.40
6-7	15158	13.50
7-8	25396	22.60
8-9	502	0.40
9-10	15176	13.50
Total	112364	



7-8 is High, 9-10 is Critical

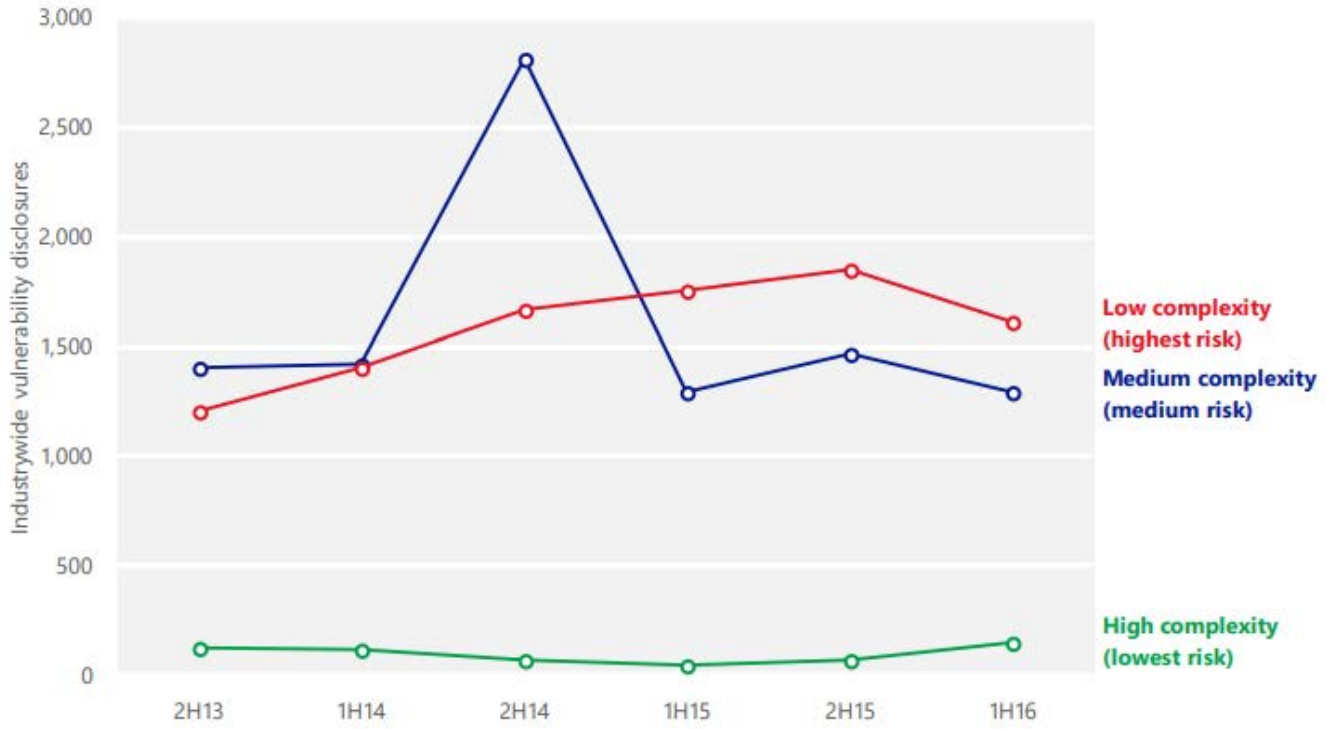
Problem – Easy to Exploit

Problem Definition –

How Did It Get This Way?

Pretty easy to exploit

- Most vulnerabilities are easy to exploit



Thousands of high criticality exploits each year x low complexity = very tough job

Problem – Competition for Resources

Problem Definition –

How Did It Get This Way?

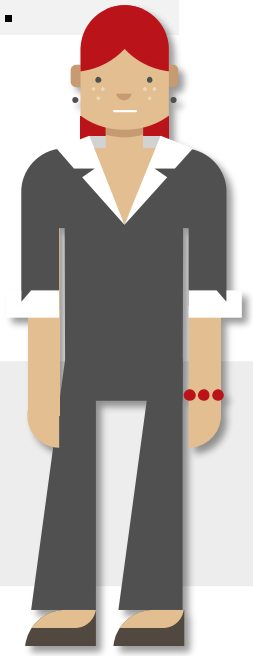
- Avalanche of New Threats
- Media- and Vendor-Driven Narratives
- Compliance Always Wins
- Too Many Projects
- Higher Priority Pet Projects/Politics
- Slower Budgeting Cycles
- Inefficient IT Organization

Problem – Humans are Poor at Risk Evaluation

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

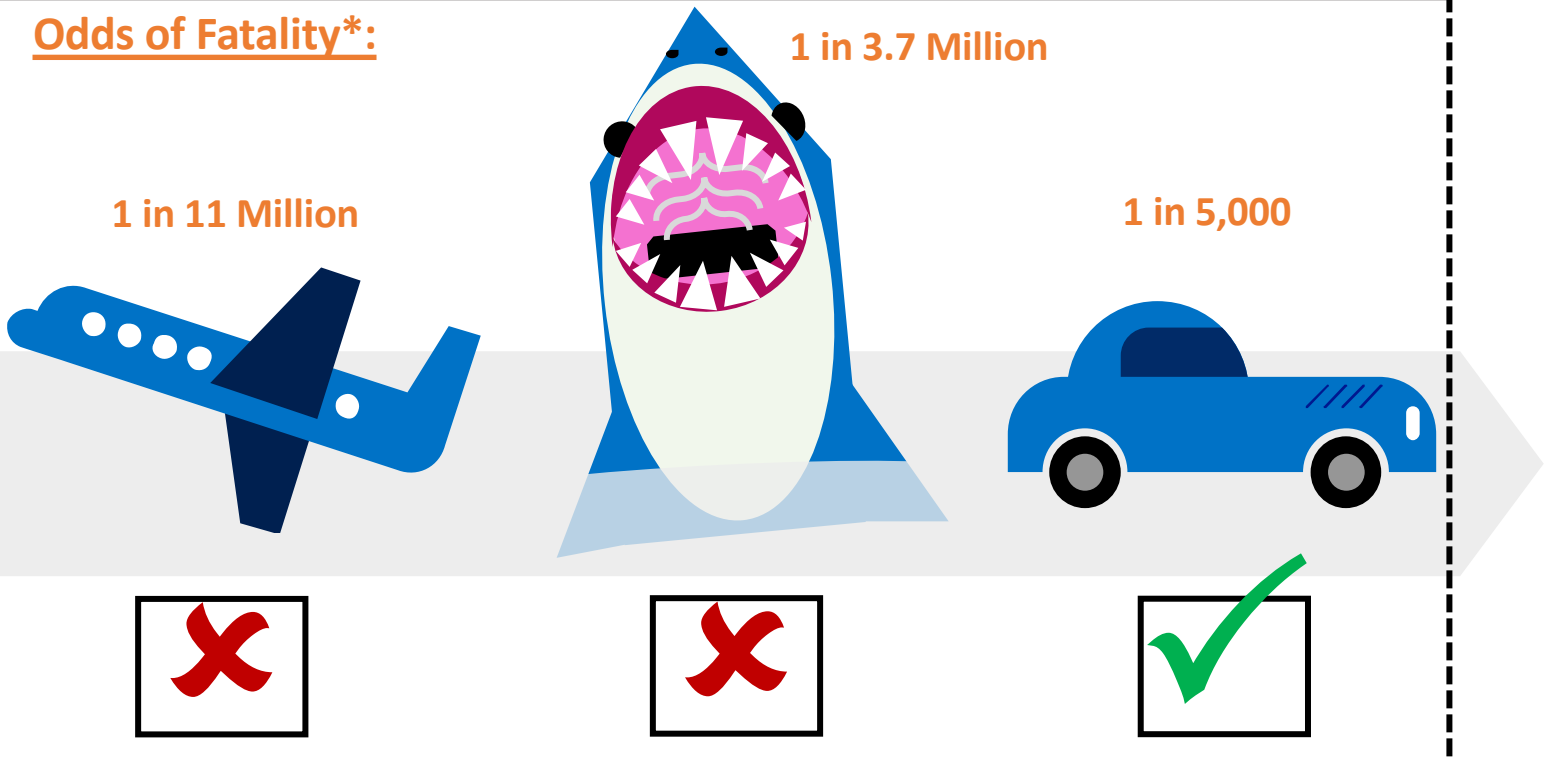
Problem Definition –

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*:



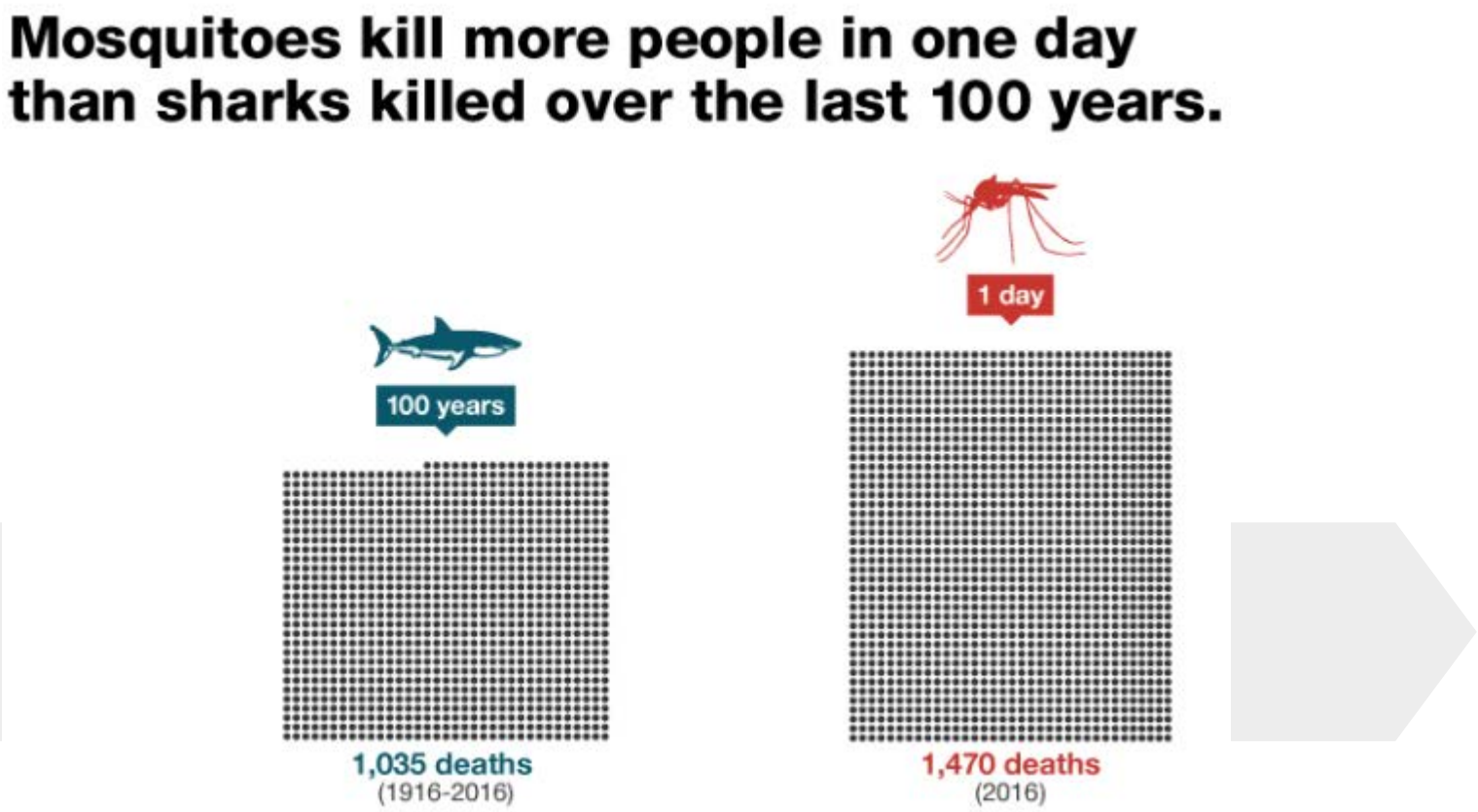
*sources: Clarke, Ropeik, National Geographic

Problem – Humans are Poor at Risk Evaluation

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

Problem Definition –

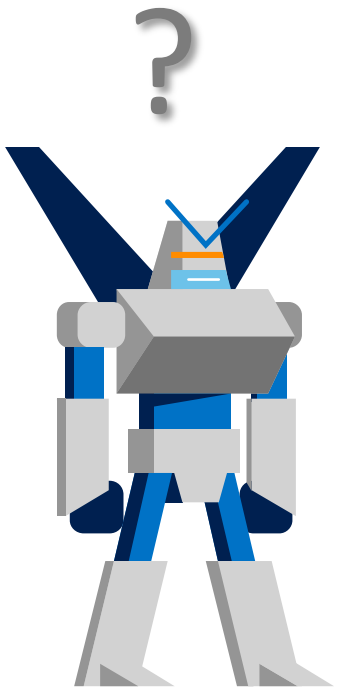
How Did It Get This Way?



Problem – Threat (Un)Intelligence

Problem Definition –

How Did It Get This Way?



Most organizations threat intelligence cannot:

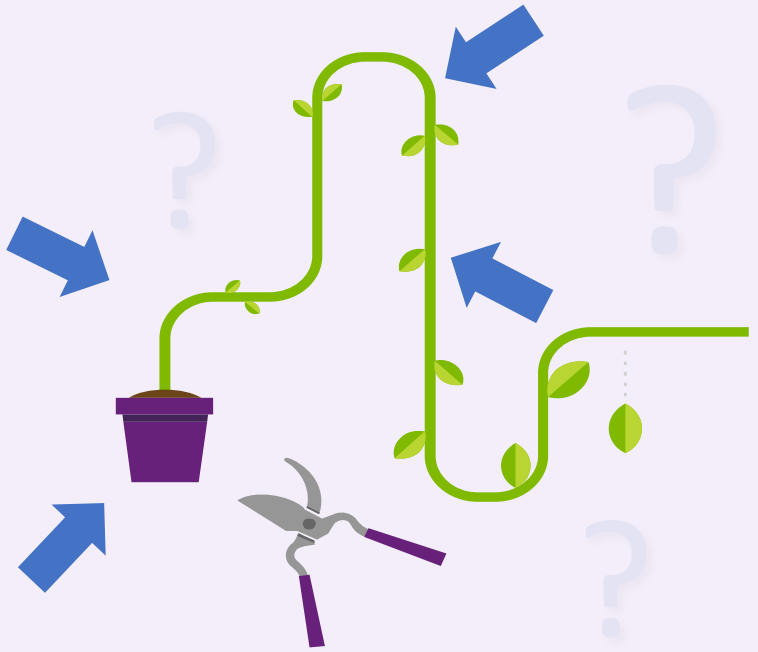
- Tell you how the organization is successfully attacked the most
- Not risk-focused
- Has or leads to inadequate threat detection
- Has or leads to little to no forensic analysis
- Often doesn't capture root causes
- Too much data, but not enough useful data
- What is accurately detected isn't effectively communicated across the entire organization

Problem – Not Enough Focus on Root Causes

root causes → how attackers/malware break in

What's the number one root cause threat in your environment?

- Programming Bug
- Social Engineering
- Authentication Attack
- Human Error
- Misconfiguration
- Eavesdropping/MitM
- Data/Network Traffic Malformation
- Insider Attack
- Reliance Issue
- Physical Attack



Ask Yourself 3 Key Questions:

1. Can your security team correctly answer what is the top root 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:

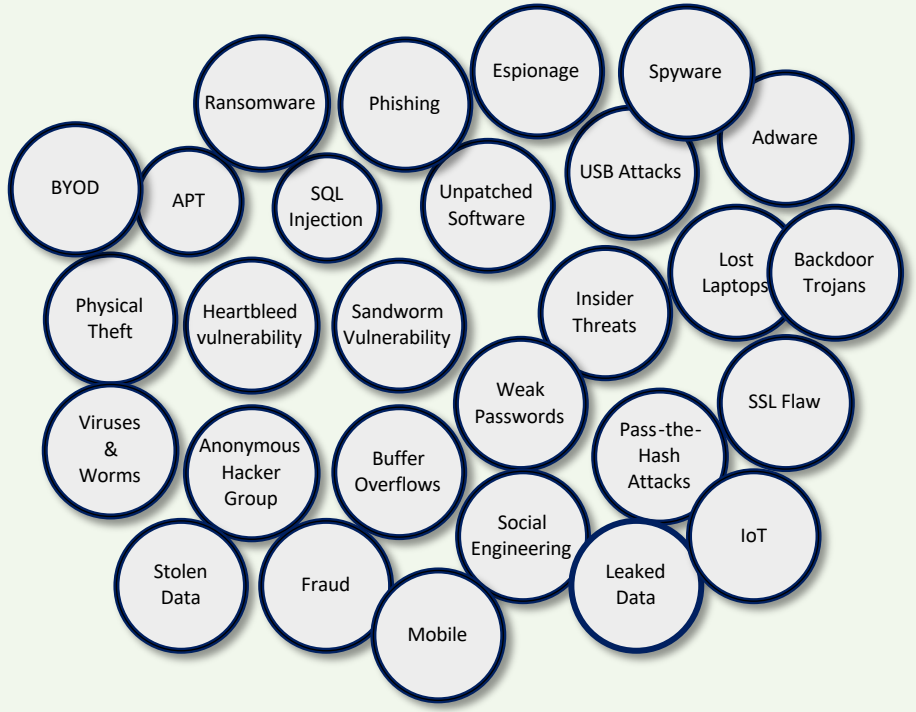
- Not ranking risks correctly relative to each other
- Seeing all risks as more equal than they are
- Focusing on the wrong threats
- Focusing on individual threats instead of more inclusive, broader root cause issues
- Belief that malicious events are impossible to stop or minimize (“assume breach”)

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

The Traditional Approach to IT Security Risks

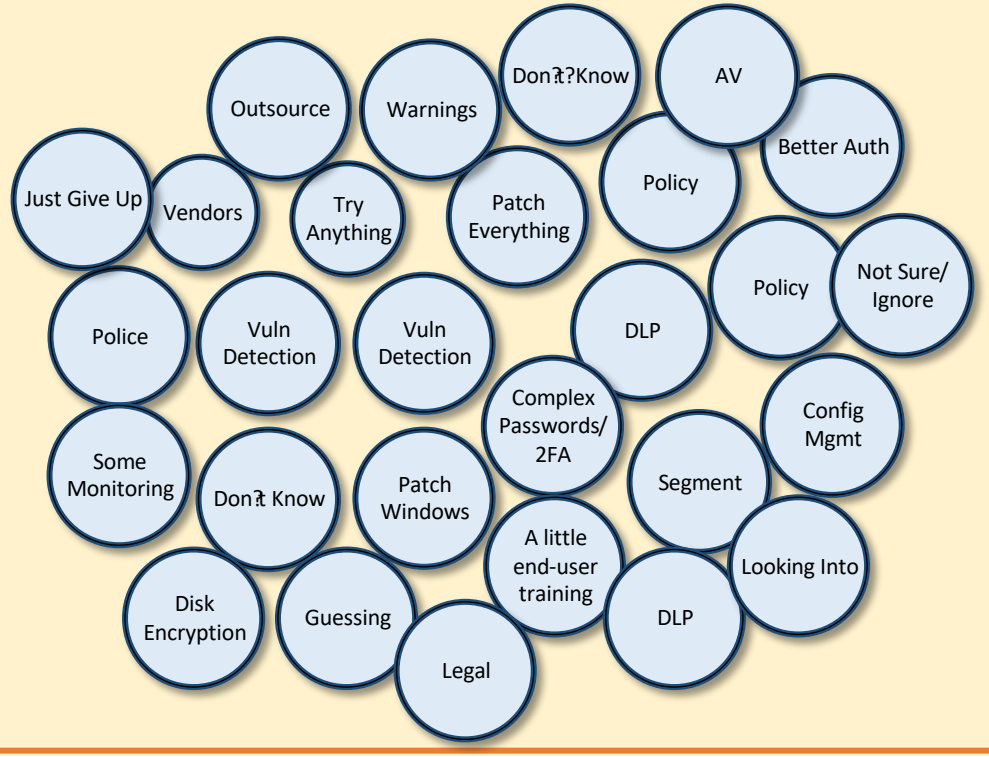
Poor risk analysis leads to mis-ranked, whack-a-mole", defenses

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: http://aka.ms/datadrivendefense

Focus on Root Causes

You should care most about root causes of initial breaches

Ransomware isn't the problem. Pass-the-hash-attacks aren't the problem

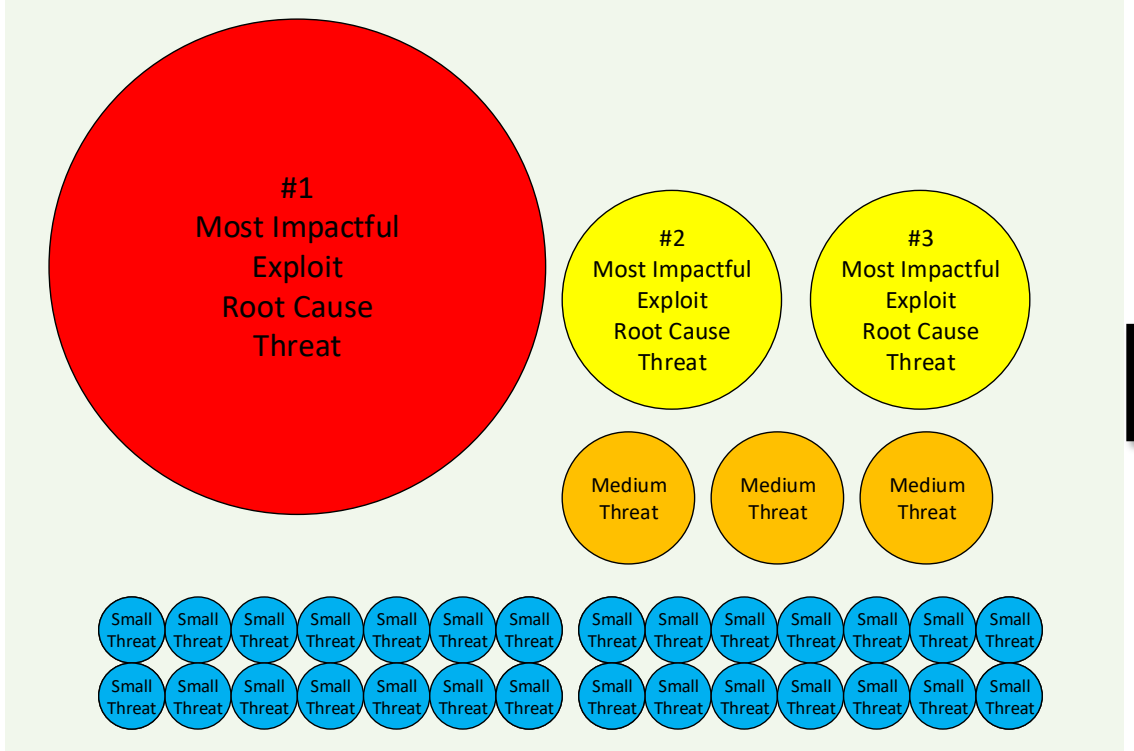
Focusing on individual threats and only what they did after they got in is like worrying about your brakes after your car is stolen

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

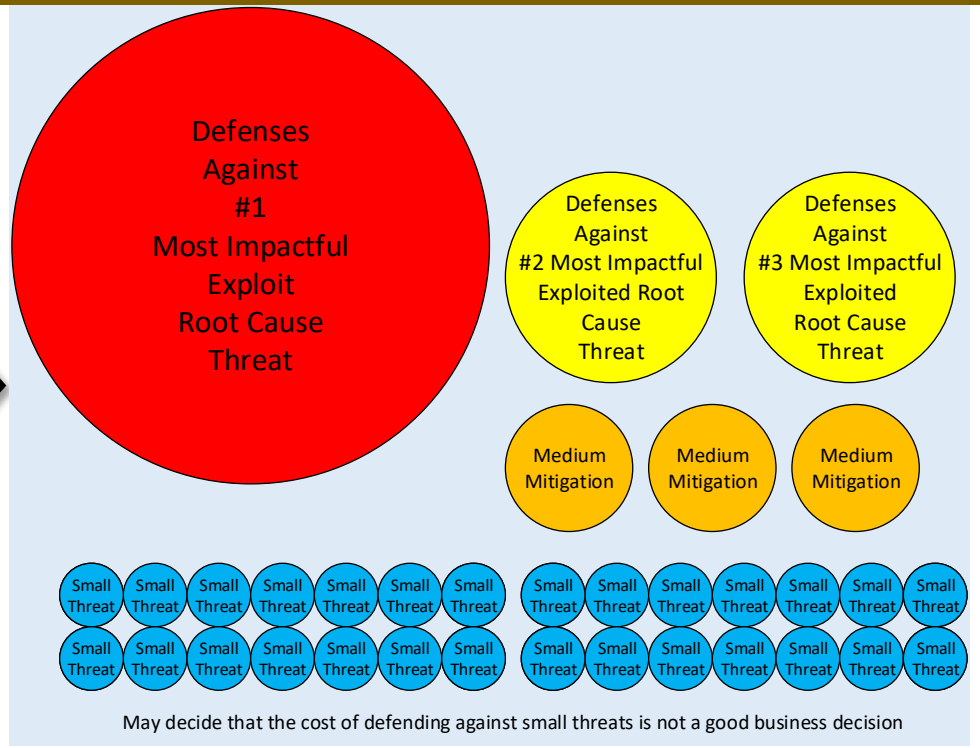
<u>Both took the same effort to get into your environment</u> and is revealing defensive gaps

The Data-Driven Defenders Approach

The Data-Driven Threat Perception



Data-Driven Defense Application



Risk Ranked Threat Perceptions:

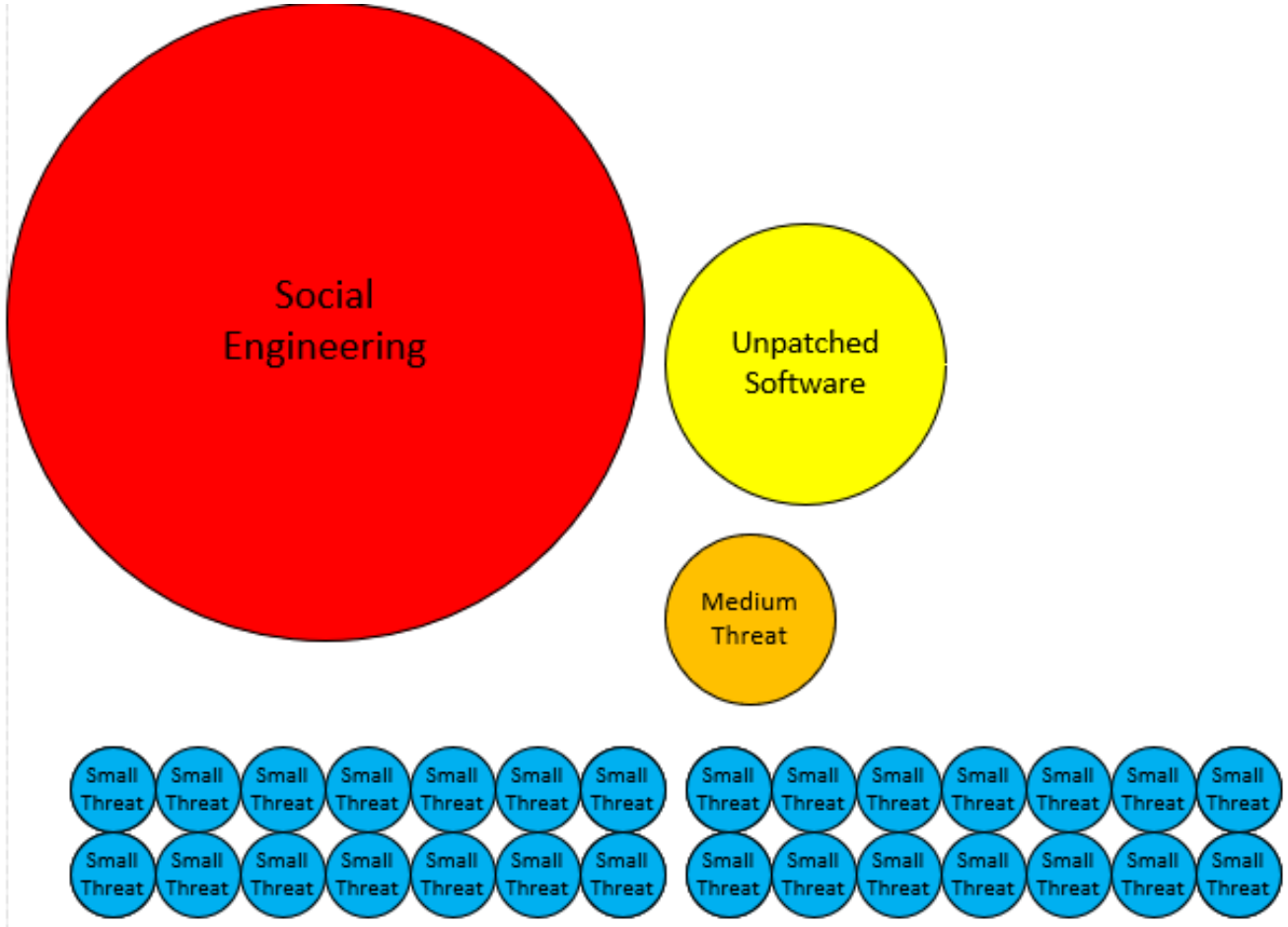
- Focuses on root causes
- Local experience and data is highly valued
- Relevance is a big deciding factor

Risk Ranked Defenses:

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

Biggest Initial Breach Root Causes for Most Companies

- Social Engineering
- Unpatched Software



Preventative Controls

- Technical
- Training

Social engineering is responsible for 70% - 90% of all malicious data breaches

Benefits of Data-Driven Computer Defense?

Benefits include:

- Increased focus on the right things
- More efficient, lower-cost, computer security defense
- Improved data collection and analysis
- Better threat intelligence
- Improved threat detection
- Quicker responses to growing threats
- Reduced damage
- More accountability
- Measurably lower computer security risk
- Increased trust in computer security defenses
- Increased morale by all stakeholders

Quiz:

Putting Your Knowledge to Use

What Are Your Top Threats?

- Ransomware
- Computer worms
- Pass-the-hash attacks
- Data theft
- Malicious email attachments
- Stolen credentials
- Lateral movement
- Trojans/backdoors
- Password guessing/hacking
- End-Users
- Poor security configurations
- Uncaring Management
- Lack of 2FA
- Rogue web sites

Trick question: Most of these are resulting outcomes from the real root causes!

What Are Your Top Threats?

Focus on Root Causes!

- Programming Bugs
- Social Engineering
- Authentication Attacks
- Eavesdropping/MitM
- Misconfigurations
- Data/Network Traffic Malformation
- Insider Attacks
- Reliance Issues
- Human Error
- Physical Attacks

Today, for most companies, the top two biggest risks, by a long shot are:

- **Unpatched software**
- **Social engineering**

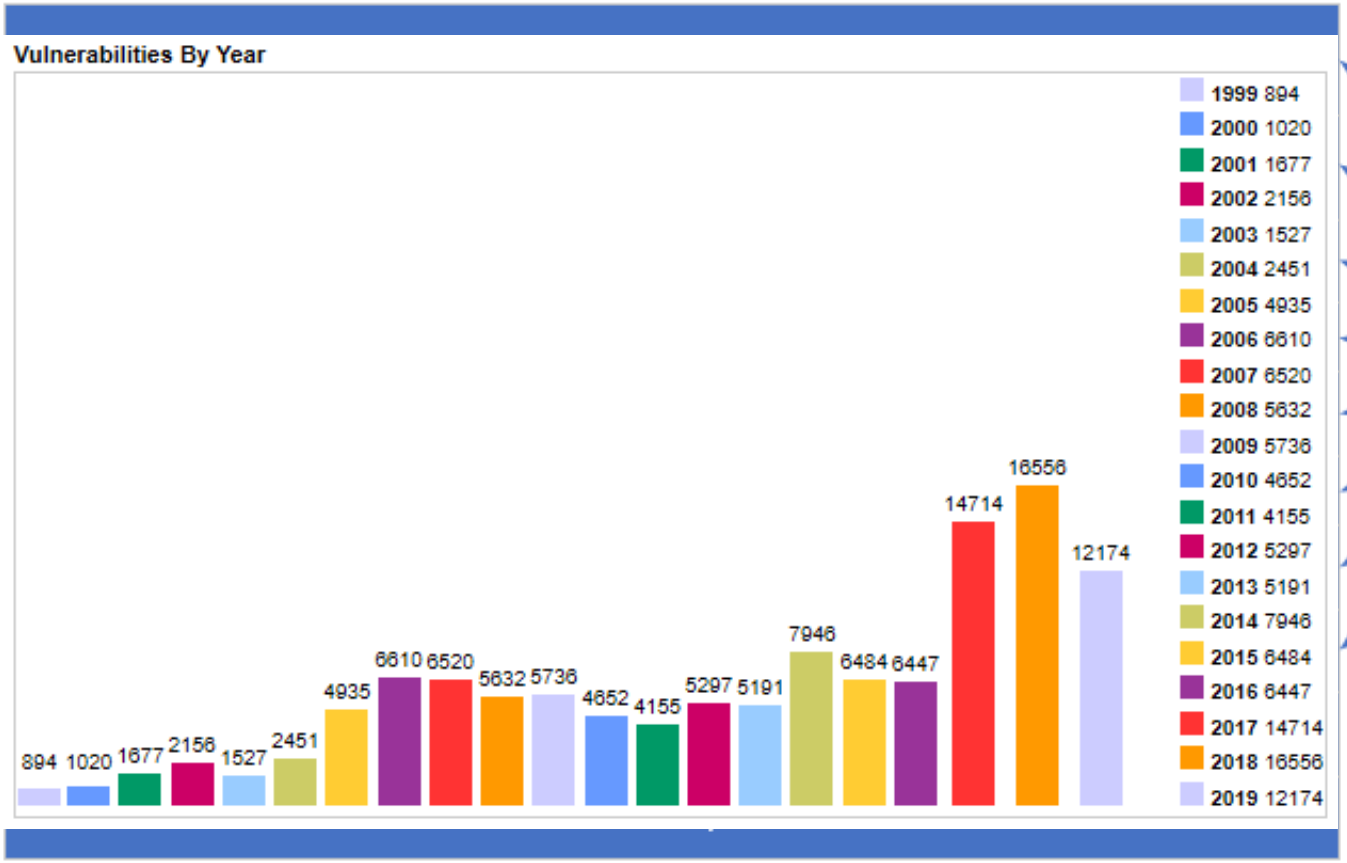
Usually less than a handful of threats compromise the vast majority of risk in most companies

What To Patch First?

Patching Scenarios

Traditional/Legacy | Hosted Virtual Machines | Containers/Microservices

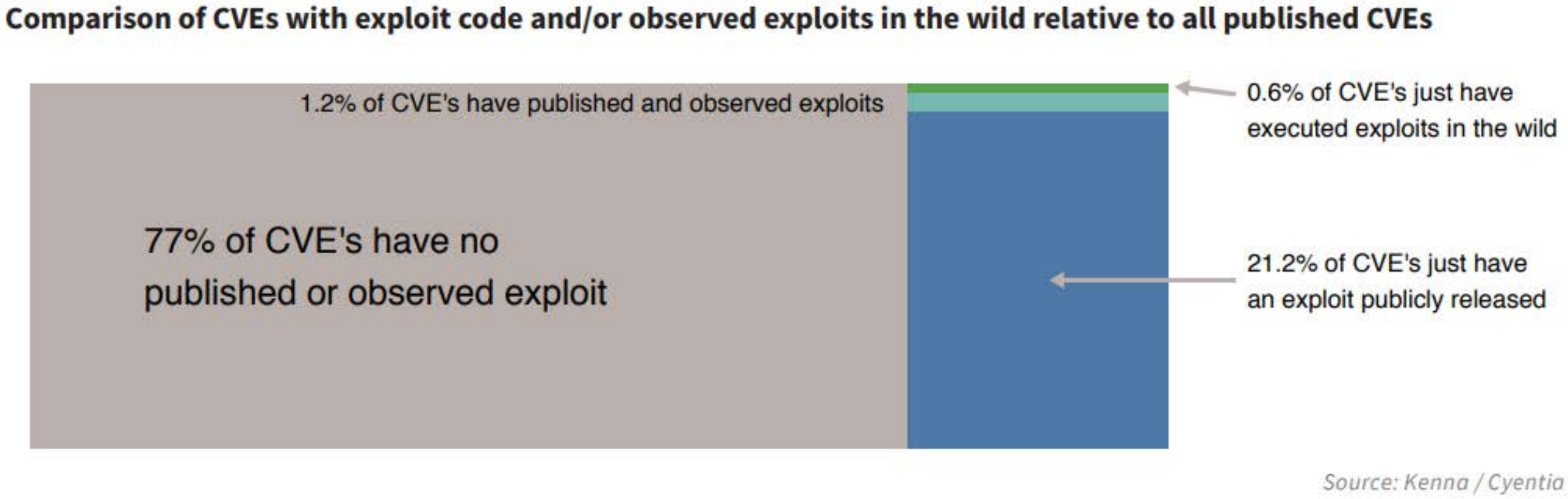
Deployment Models/Layers



Patch Here

Focus on Current and Most Likely Future Threats

Less than 2% of CVEs get exploited in the wild!



But even this isn't focused enough!

Top Software Vulnerabilities

Usually less than a handful of threats compromise the vast majority of real risk

Most attacked unpatched software is usually, **Internet-facing/accessing** and:

Clients

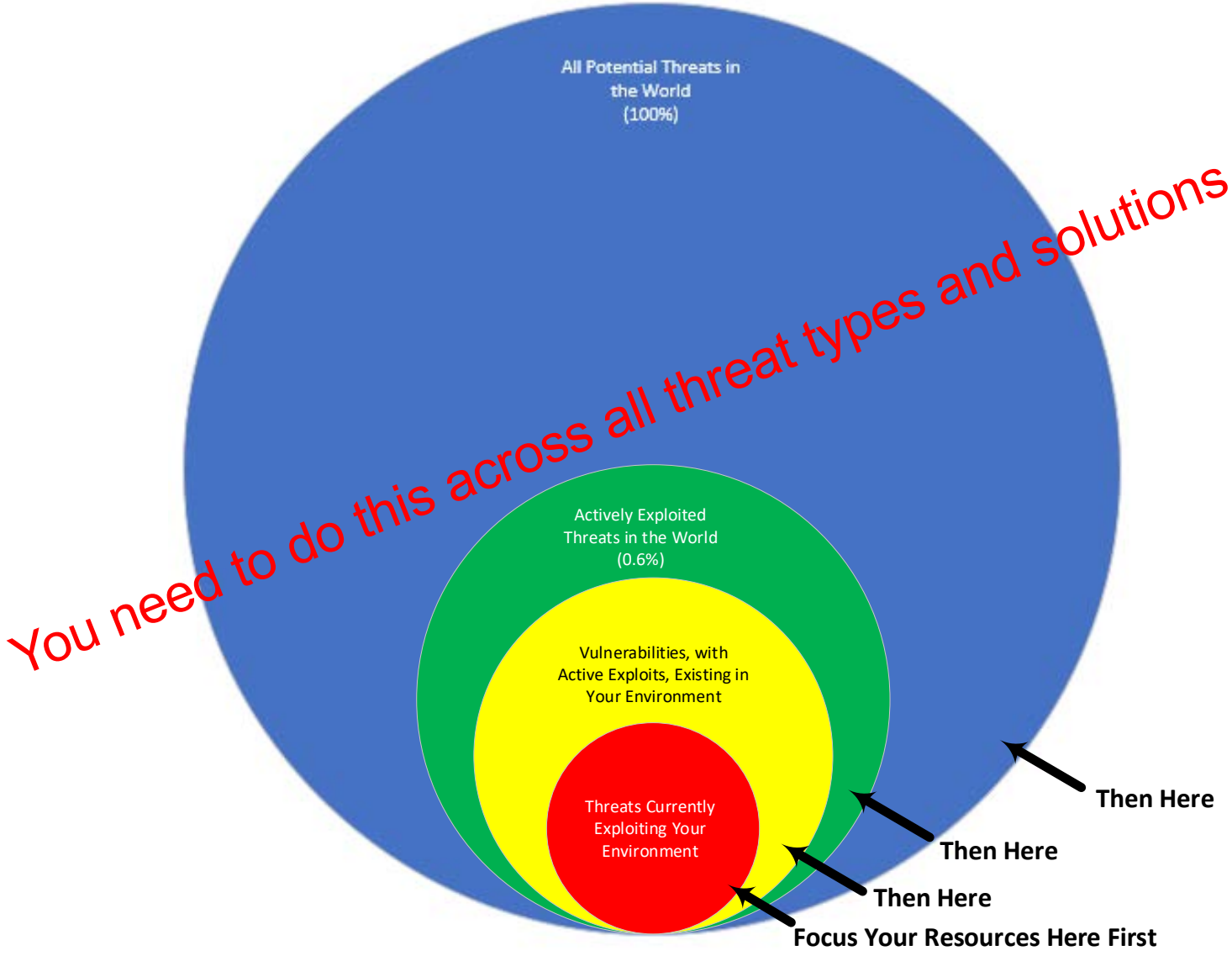
- **Browser Add-Ons**
- **Network-advertising Services/Daemons**
- **OS**
- **Productivity apps (Microsoft Office, etc.)**

Servers

- **Web server software**
- **OS**
- **Database**
- **Mgmt software**

What are your top unpatched threats?

What to Patch First and Best?



Top Vulnerabilities

Usually less than a handful or two of threats compromise the vast majority of real risk

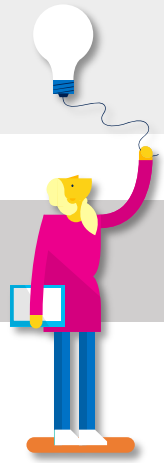
Concentrate on, in order of importance:

- **Exploits Actively Successfully Used Against You**
- **Exploit Likely to Be Used Against Successfully You In the Near Future**
- **Exploit Used Successfully Against You In the Recent Past**

Everything Else

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

What are your top unpatched threats?



Patching Threat vs. Risk

There is a big difference between your most unpatched program and your biggest risk

Example
For a decade, Microsoft's Visual C++ Redistributable was the most unpatched program

However:
- **It was never hacked in the wild**
- **Rarely callable within a browser session (i.e. client-side exploit)**
- **It wasn't a "listening service"**
- **It usually didn't have System or admin access**
- **It was installed in different places by each relying vendor**
- **No public exploit code**

- **Just because it is your biggest risk doesn't mean it is actually attacked the most**

What are Your Top Social Engineering Threats?

Usually less than a handful or two of threats compromise the vast majority of real risk

Social Engineering Threats

- **Email-based**
- **Web-based**
- **Social Media-based**
- **Transfer Money Requests**
- **Phone-based, SMS-based, etc.**

- **How to fight? Social Awareness Training, Technical**

What are your top social engineering threats?

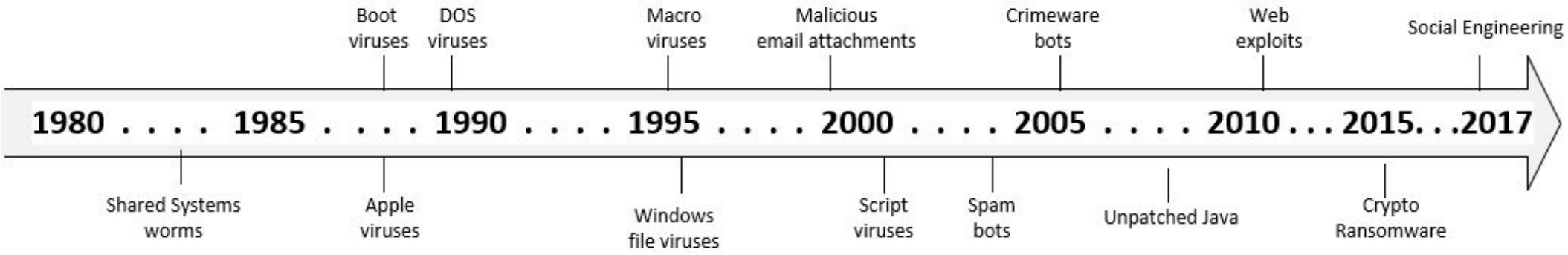
Focus on Better (Local) Threat Intelligence

Focus Prioritization:

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

"The Main Driver is Local Threat Intelligence"

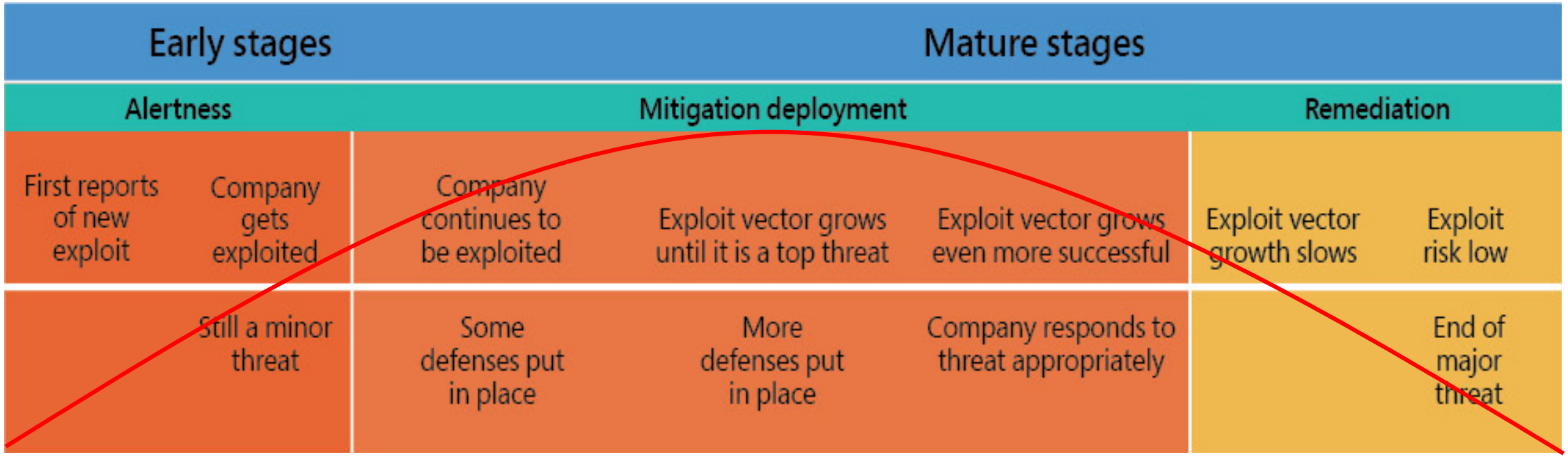
Top Exploits Change Over Time



Exploit popularity always changes over time

But how we respond to them doesn't

Computer Security Defense Response Cycle



We move from unaware, to underestimating impact, to finally addressing it

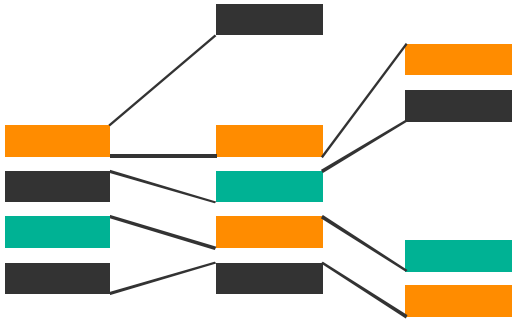
You need to do this across all threat types and solutions

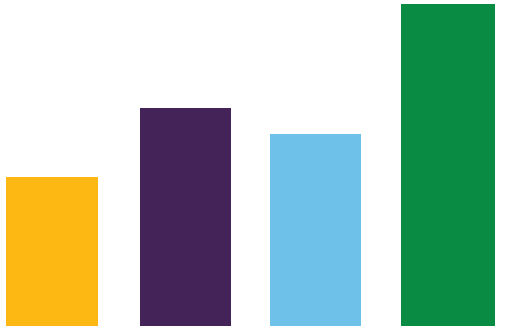
Goal: Recognize emerging, growing threats faster so you can react quicker

Getting a Faster Response Cycle

Use your data and metrics to:

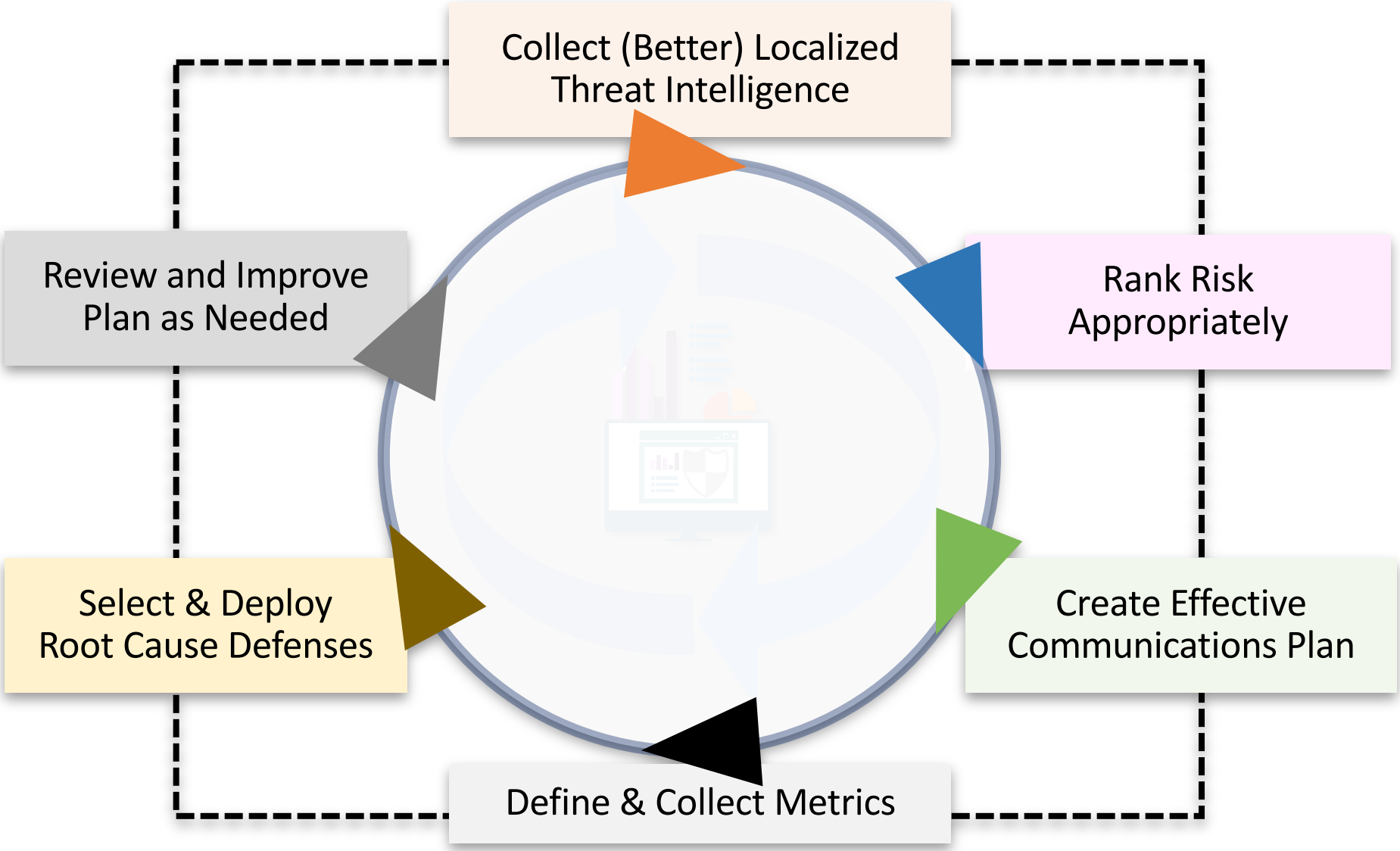
- Get faster detection/early warning
- Measure exploits success in your organization
- Measure trends over times





Increasing trends require better responses

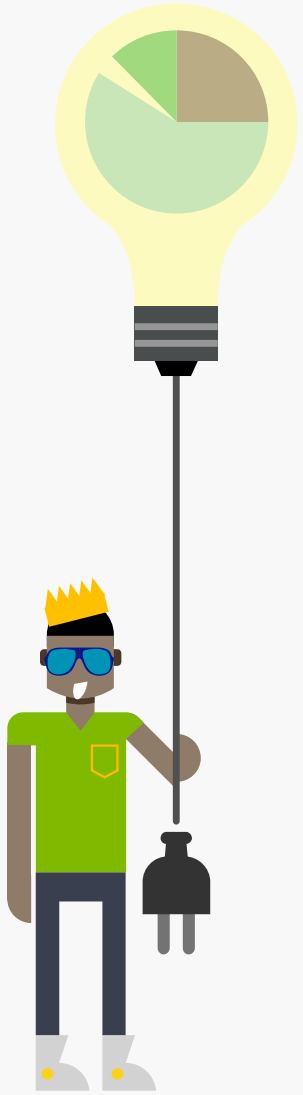
The Data-Driven Defense Planning Cycle



Some 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
- Everyone understands biggest attacks and threats
- Your defenses are right-aligned against your biggest threats
- Specific patch teams (three programs instead of all)
- No un-ranked IT security lists anymore!
- Collect the right data (ex. mean time to detect, AppLocker)
- Social engineering training – more than 30 minutes a year

How To Implement a Data-Driven Defense?

- Evangelize this concept! Use book, white paper, and slides
- Get a computer security data analytics person or team
- Collect all your data into single places for more aggressive data analysis
- Figure out what questions to ask
- Assess your threat intelligence information collection and how valid and specific it is for your organization
- Figure out your top root causes and threats
- Assess how well your threat intelligence and defenses align to those threats
- Fill in the gaps
- Make aligned defenses measurable and accountable
- Need more help? Email me at rogerg@knowbe4.com

Resources

Free IT Security Tools

- Domain Doppelgänger
- Awareness Program Builder
- Domain Spoof Tool
- Mailserver Security Assessment
- Phish Alert
- Ransomware Simulator
- Weak Password Test
- Phishing Security Test
- Second Chance
- Email Exposure Check Pro
- Training Preview
- Breached Password Test

12+ Ways to Hack Two-Factor

All multi-factor authentication (MFA) mechanisms can know how to defend against MFA hacks? This whitepa those attacks.

Whitepapers

Ransomware Hostage Rescue Manual

Get the most complete Ransomware Manual packed with actionable info that you need to have to prevent infections, and what to do when you are hit with ransomware.

CEO Fraud Prevention Manual

CEO fraud is responsible for over $3 billion in losses. Don't be next. The CEO Fraud Prevention Manual provides a thorough overview of how executives are compromised, how to prevent such an attack and what to do if you become a victim.

» Learn More at www.KnowBe4.com/Resources «

Thank You!

Questions?

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