AFRICA CYBER SECURITY
CULTURE CONFERENCE

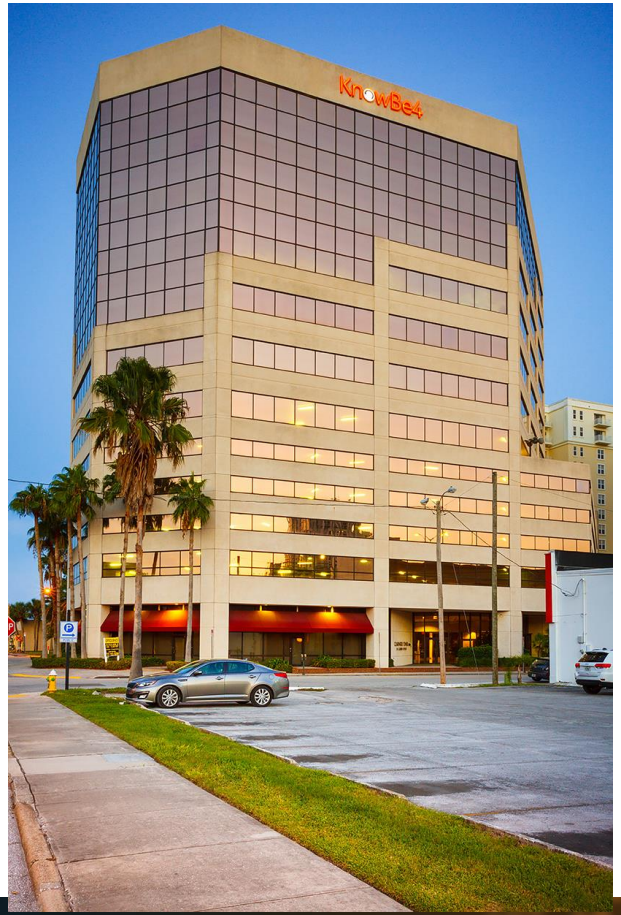
Creating Your Best Data-Driven Defense

ROGER A. GRIMES

rogerg@knowbe4.com

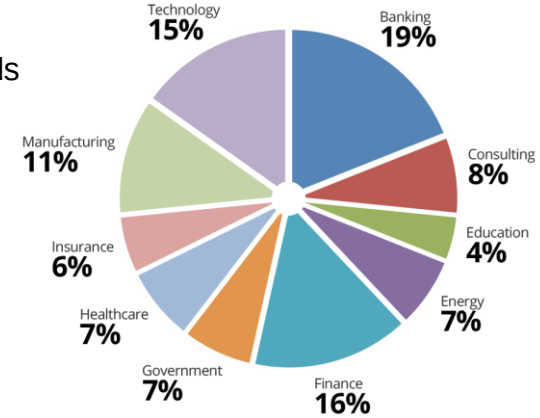
KnowBe4

Human error. Conquered.



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



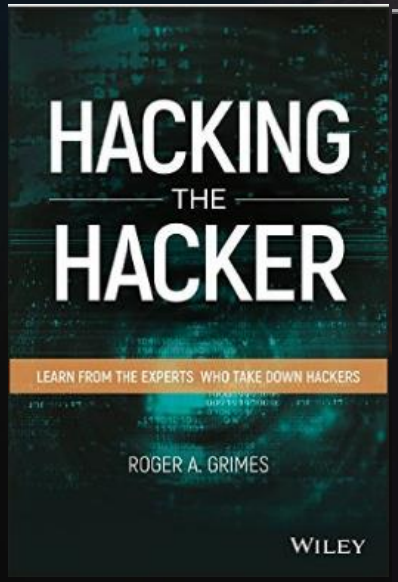
About Roger

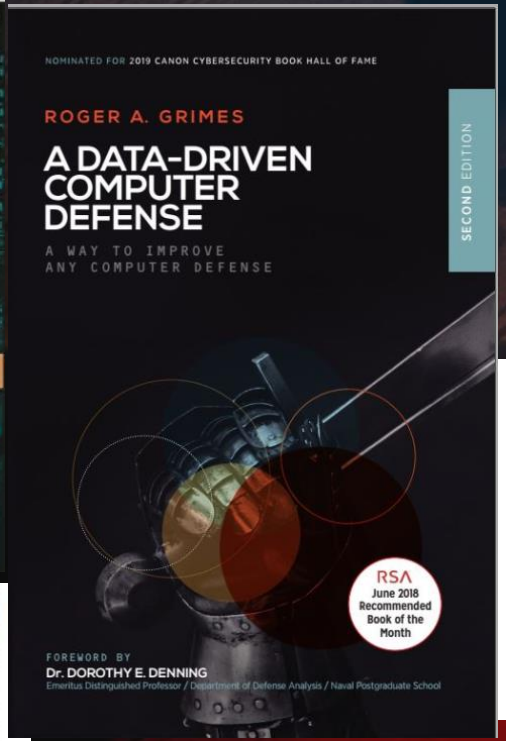
- 30 years plus in computer security
- Expertise in host and network security, IdM, crypto, PKI, APT, honeypot, cloud security
- Consultant to world's largest companies and militaries for decades
- Previous worked for Foundstone, McAfee, Microsoft
- Written 12 books and over 1,000 magazine articles
- *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)

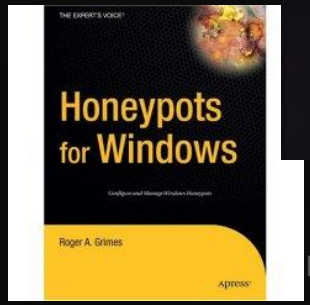
Certification exams passed include:

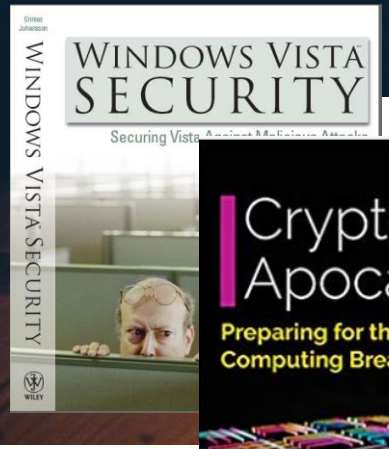
- CPA
- CISSP
- CISM, CISA
- MCSE: Security, MCP, MVP
- CEH, TISCA, Security+, CHFI
- yada, yada

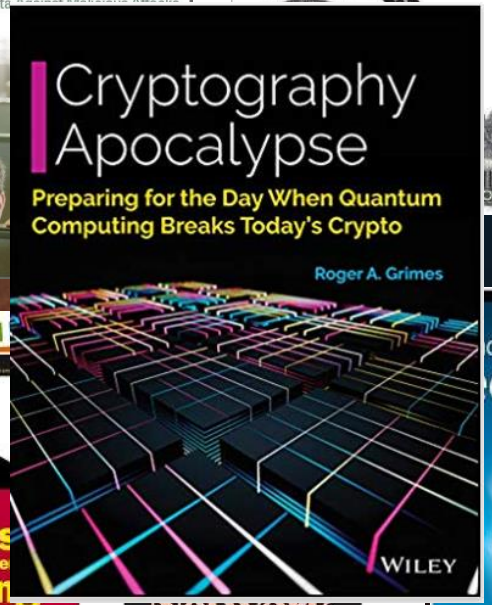
Roger's Books

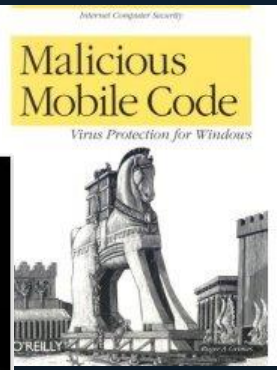


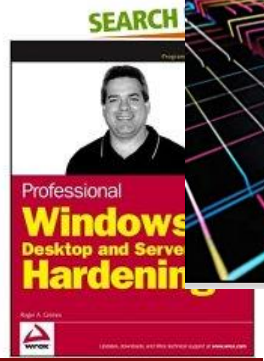


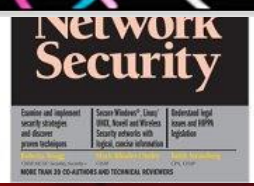


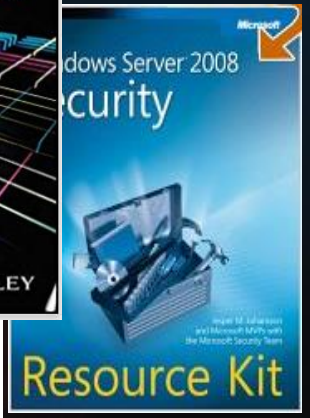












https://www.amazon.com/Data-Driven-Computer-Defense-Way-Improve/dp/1092500847/

Today’s Presentation

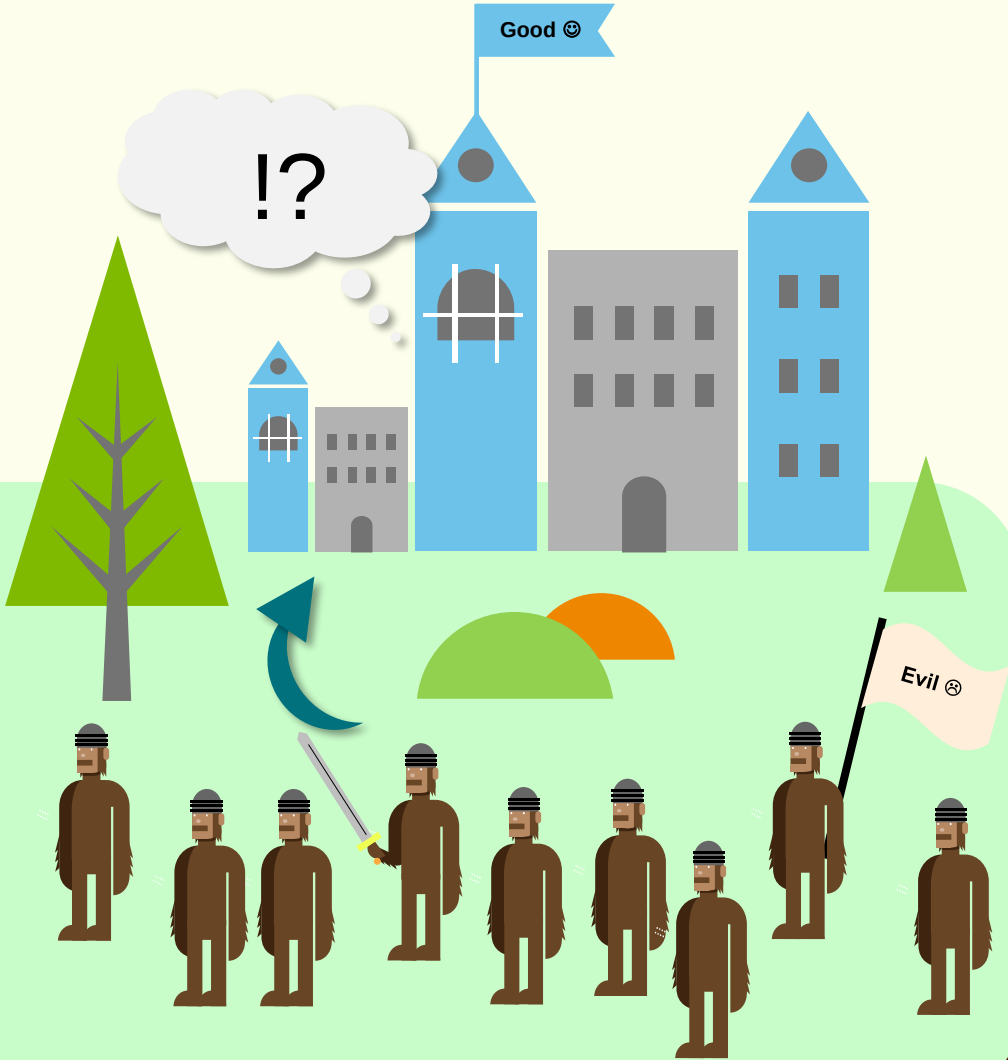
- How to Have a More Efficient, Better, Cost-Effective Defense
- The Biggest Problem With Most Computer Defenses
- How it Got This Way
- How to Fix

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 right flank of battle
- Good side responds by building up left 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?

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

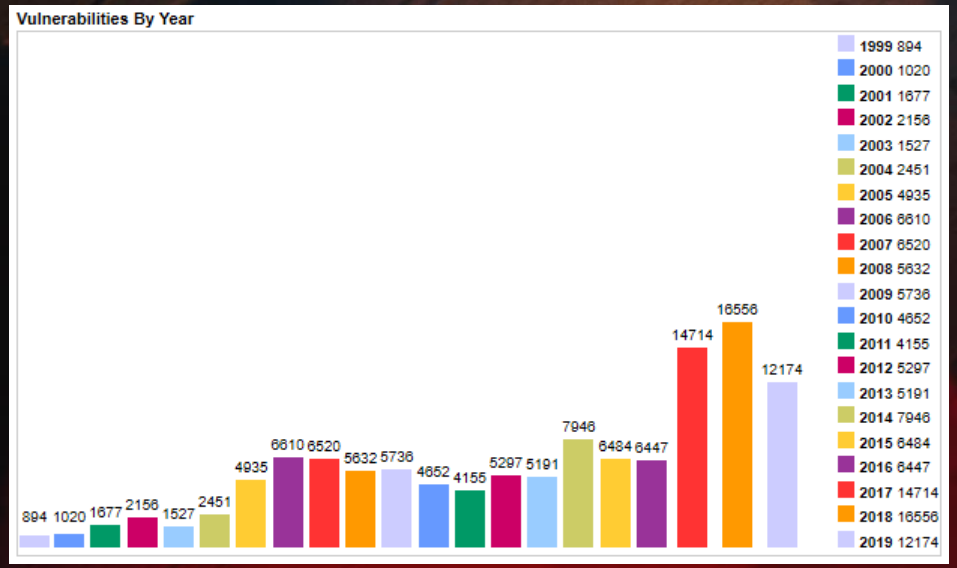
Problem Definition –

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 –

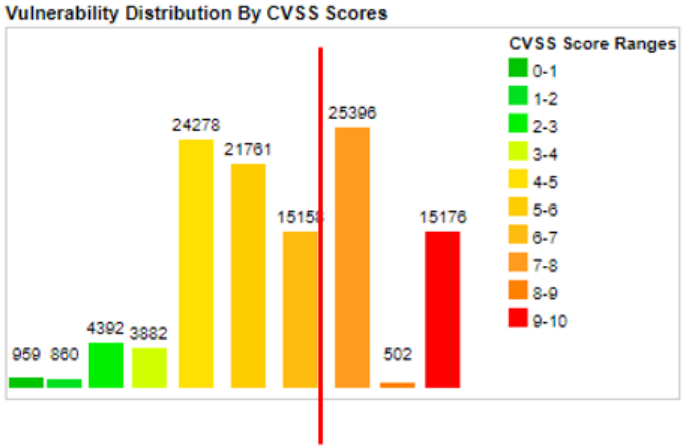
How Did It Get This Way?

That means thousands of high risk vulnerabilities a year

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

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

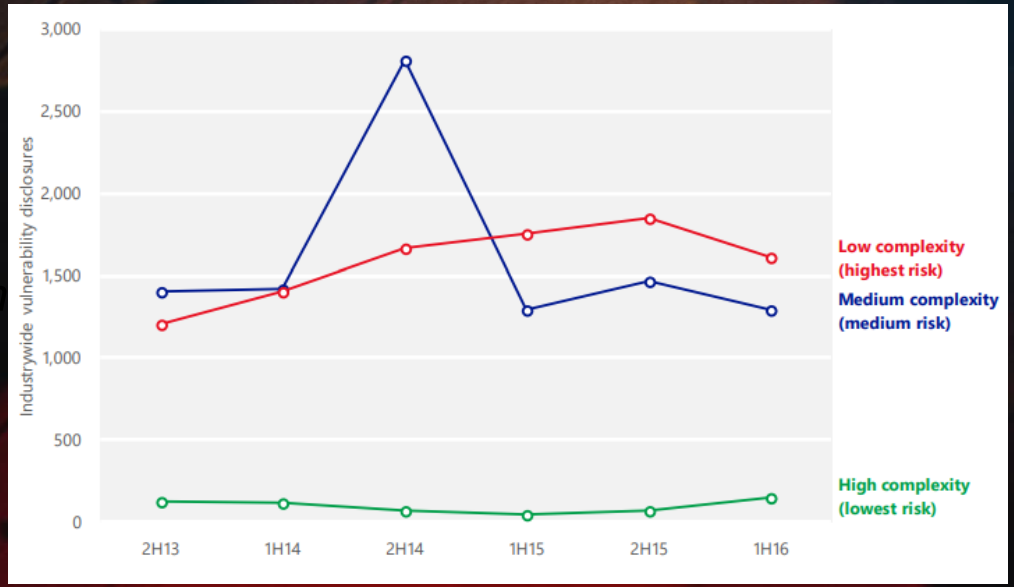
Problem Definition –

How Did It Get This Way?

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

Pretty easy to exploit

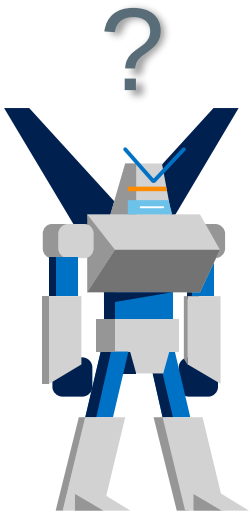
- Most vulnerabilities are easy to exploit



Problem – Threat (Un)Intelligence

Problem Definition –

How Did It Get This Way?



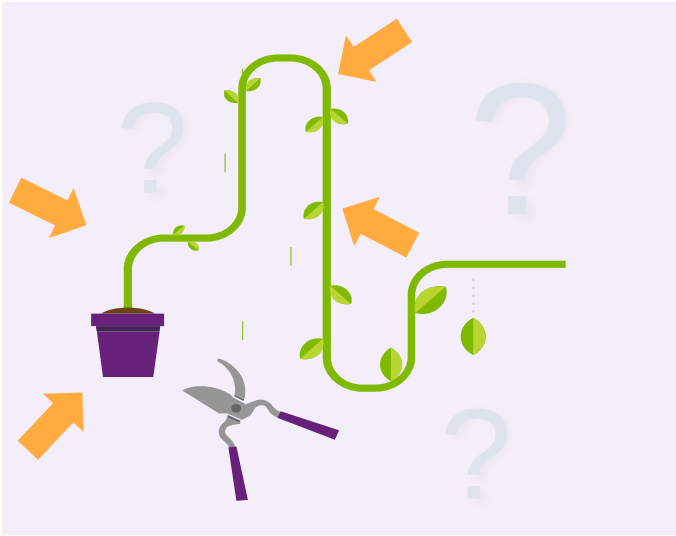
Most organizations threat intelligence:

- Cannot tell you how the organization is successfully attacked the most
- Not risk-focused
- Often doesn't capture root causes
- Has or leads to inadequate threat detection
- Has little to no forensic analysis for most threats
- 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

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
- 3rd Party Reliance Issue
- Physical Attack



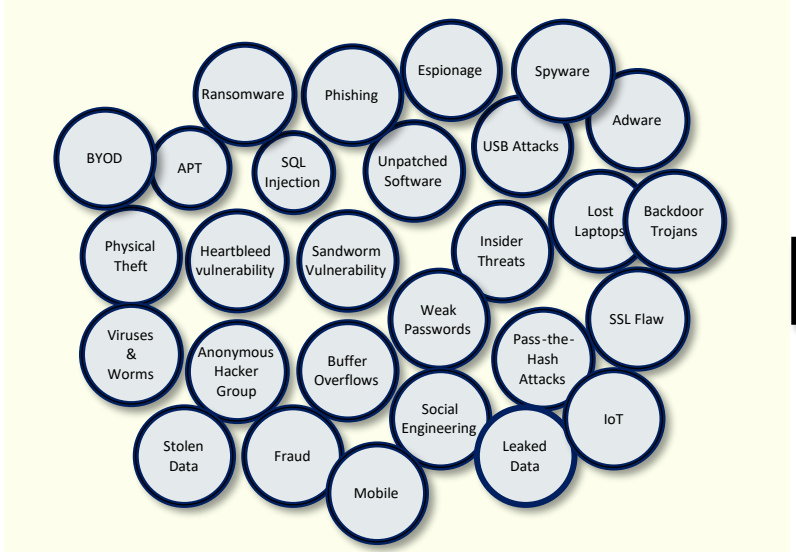
Ask Yourself 3 Key Questions:

1. Can your 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?

The Traditional Approach to IT Security Risks

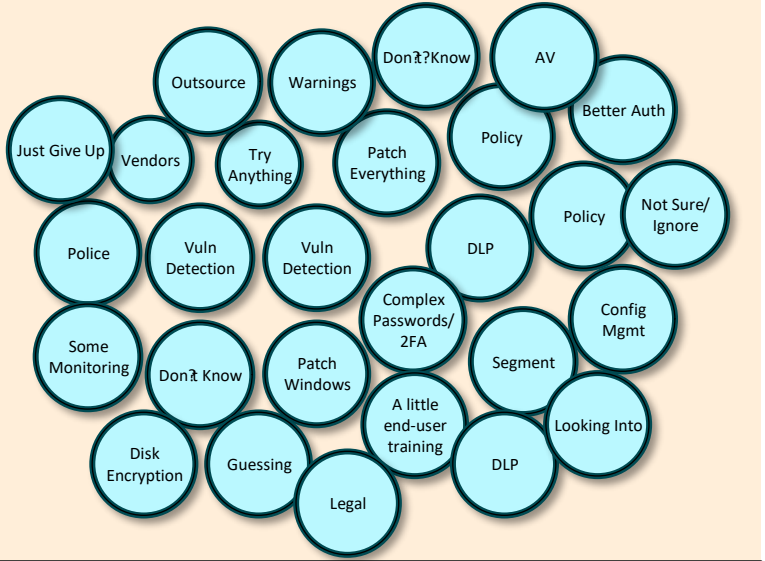
Poor risk analysis leads to mis-ranked, whack-a-mole", defenses

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

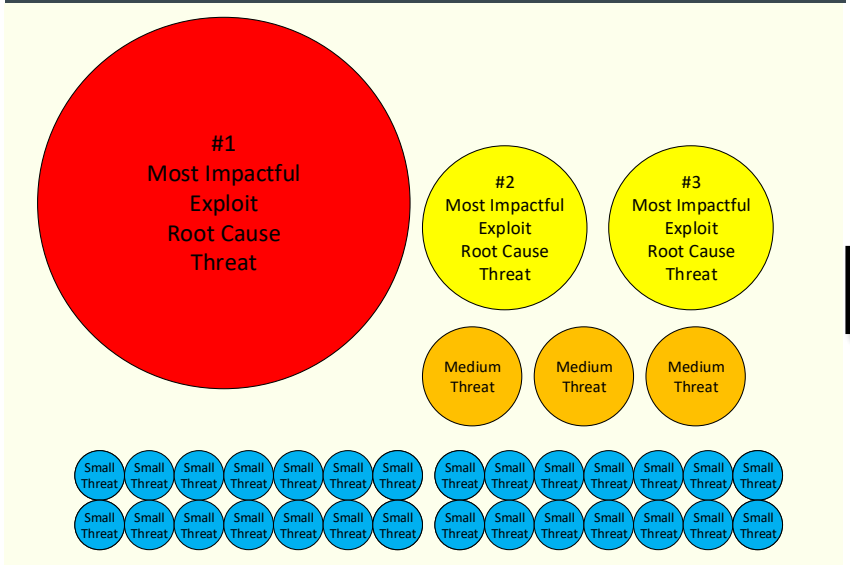
Focusing on individual threats and only what they did after they got in is like worrying about your brakes after your car is stolen

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

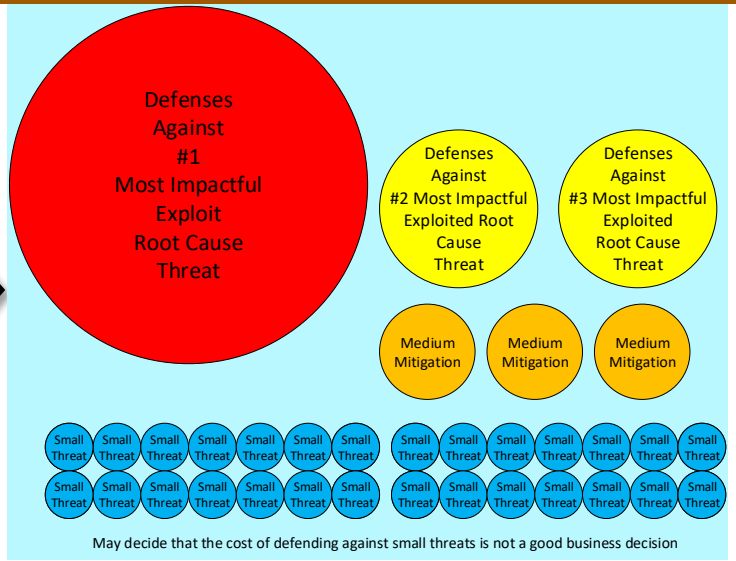
Both took the same effort to get into your environment and is revealing defensive gaps

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:

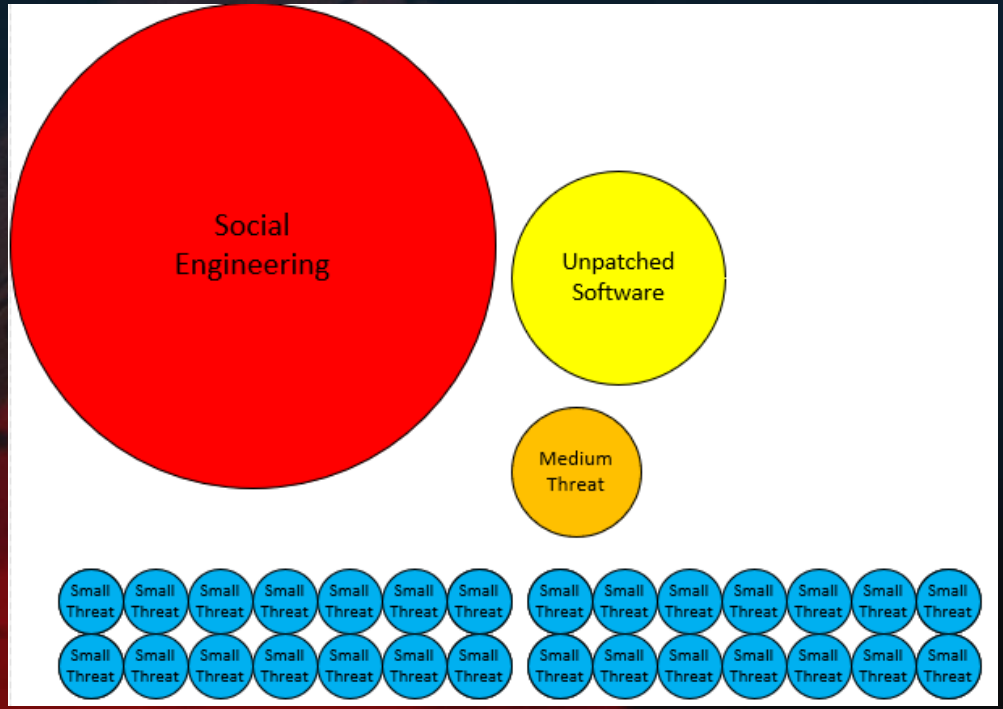
- Mitigates root causes, not individual threats
- More efficient resource utilization
- Allows clearer cost/benefit considerations

Biggest Initial Breach Root Causes for Most Companies

- Social Engineering
- Unpatched Software

<u>Preventative Controls</u>

- Policy
- Technical
- Training



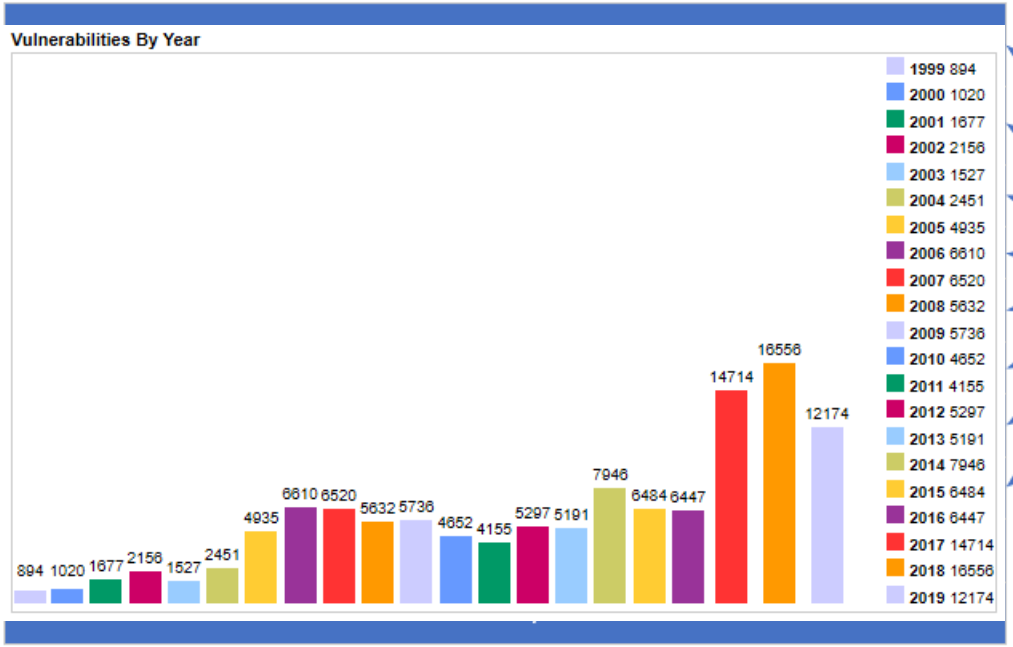
Social engineering is responsible for 70% - 90% of all malicious data breaches

What To Patch First?

Patching Scenarios

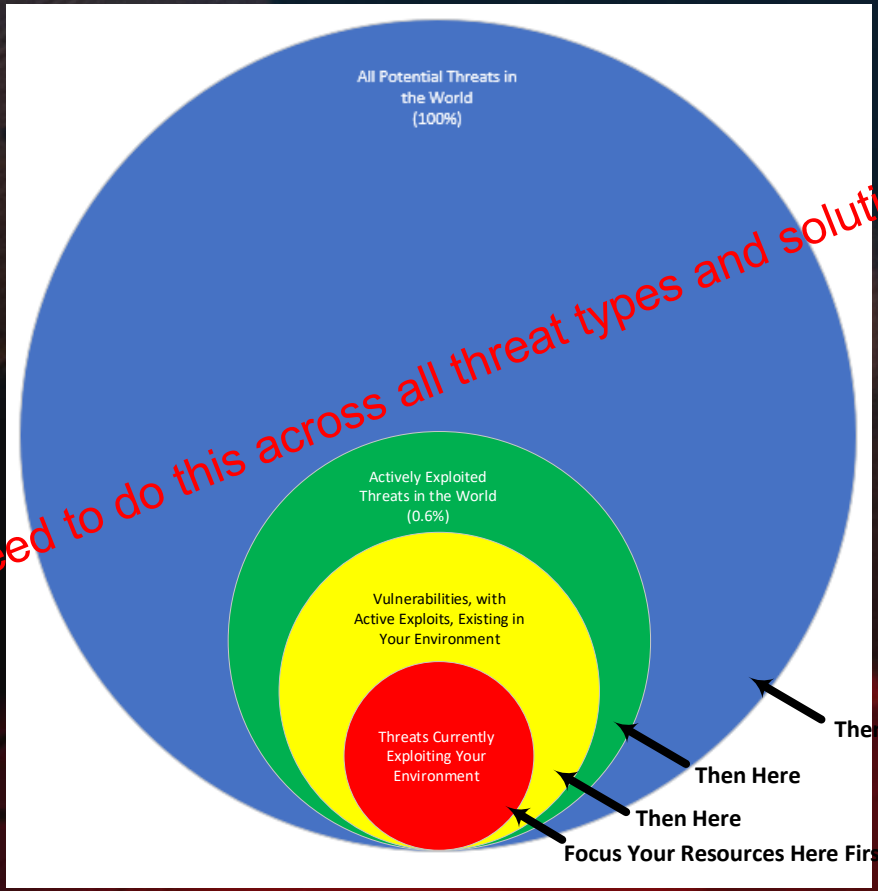
Traditional/Legacy Hosted Virtual Machines Containers/Microservices

Deployment Models/Layers



Patch Here

What to Patch First and Best?

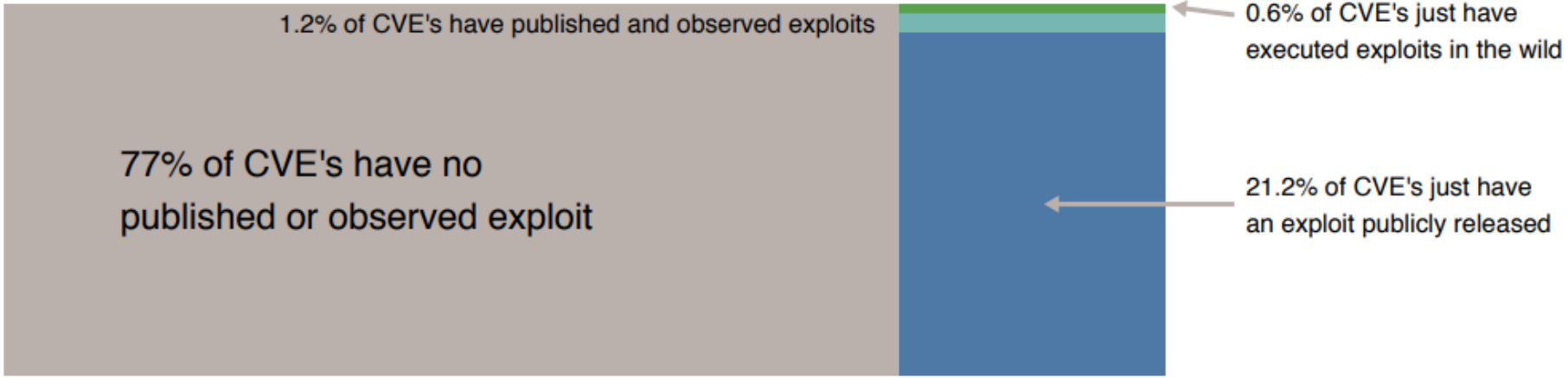


You need to do this across all threat types and solutions

Focus on Current and Most Likely Future Threats

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

Comparison of CVEs with exploit code and/or observed exploits in the wild relative to all published CVEs



Source: Kenna / Cyentia

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?

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

<u>Everything Else</u>

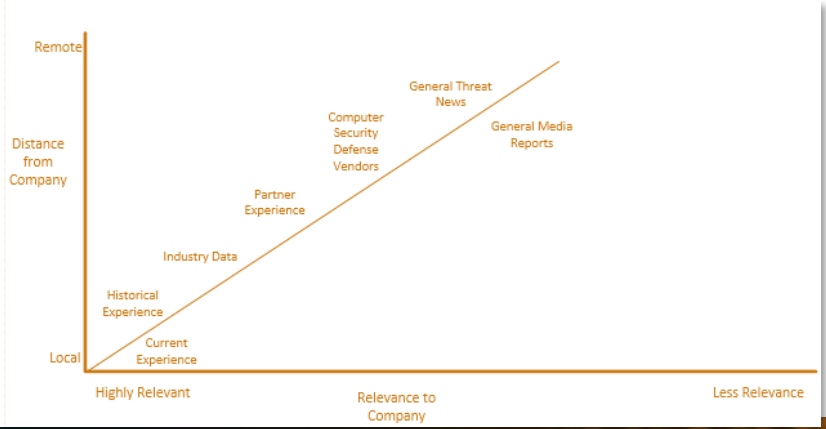
- **Widely Used Current In-the-Wild Exploits**
- **Public Exploits Announced**
- **Patch Announced, Likely to be Exploited**

What are your top unpatched threats?

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”

Resources

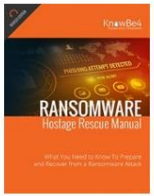
Free IT Security Tools

- 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 «

Thanks! Questions?

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