Secureworks®

Cybersecurity Technologies. Services. Solutions.

Back to Basics:

Why buying the next big thing may not help you reduce risk.

Ryan Alban

Principal, Security Solutions

in CISSP GISP

in·for·ma·tion se·cu·ri·ty

[InfoSec]

NOUN

the state of being protected against the unauthorized use of information, especially electronic data, or the measures taken to achieve this.

"the growing use of mobile applications is posing a risk to information security"

- Oxford Dictionaries

Cyber-Security is Hard

Authorized User		Threat Actor
Uses the VPN to work remotely.	→	Deploys a RAT to exfiltrate data.
Installs iTunes to backup an iPhone	→	Installs XMRig to mine Monero
Uses SCCM to deploy software updates.	→	Uses GPO to deploy software that ransoms computers and files.

Cyber-Security is Hard

Cyber-Security Team		Business Leaders
Let's deploy Multi-Factor Auth!	→	That's too inconvenient for users.
We should teach our people about phishing!	→	Everyone is busy, is it really worth the time?
Our prod e-com site is mining crypto for North Korea!	→	Downtime will cost the business $250K in lost revenue…

in·for·ma·tion se·cu·ri·ty

[InfoSec]

NOUN

A profession that turns normal people into whiskey drinking, swearing, paranoid, disheartened curmudgeons with no hope for the future of computers or humanity.

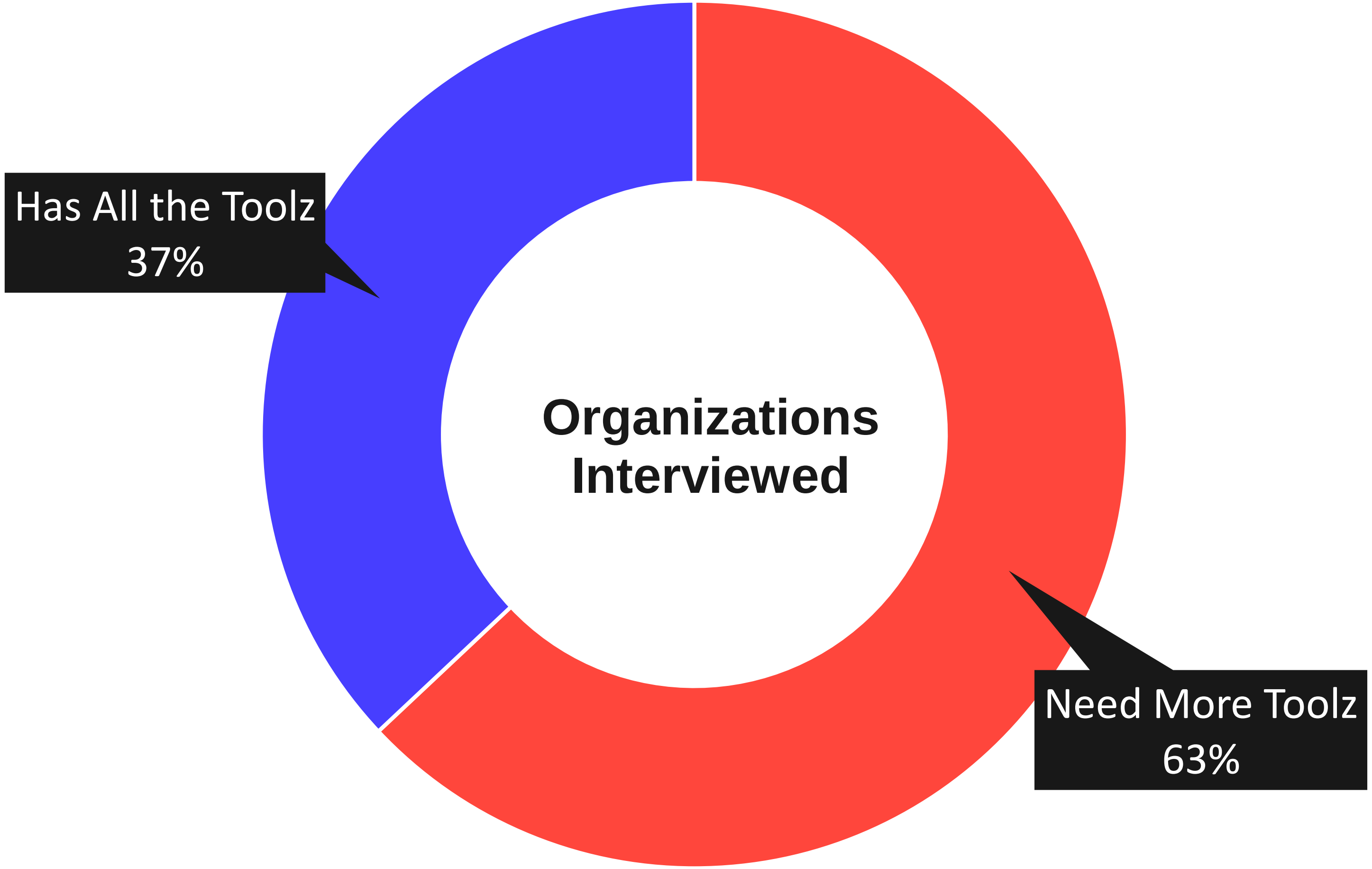
“Hi, I work in Infosec. Please pass the whiskey. No, I won't fix your computer.”

- Urban Dictionary (@mzbat)

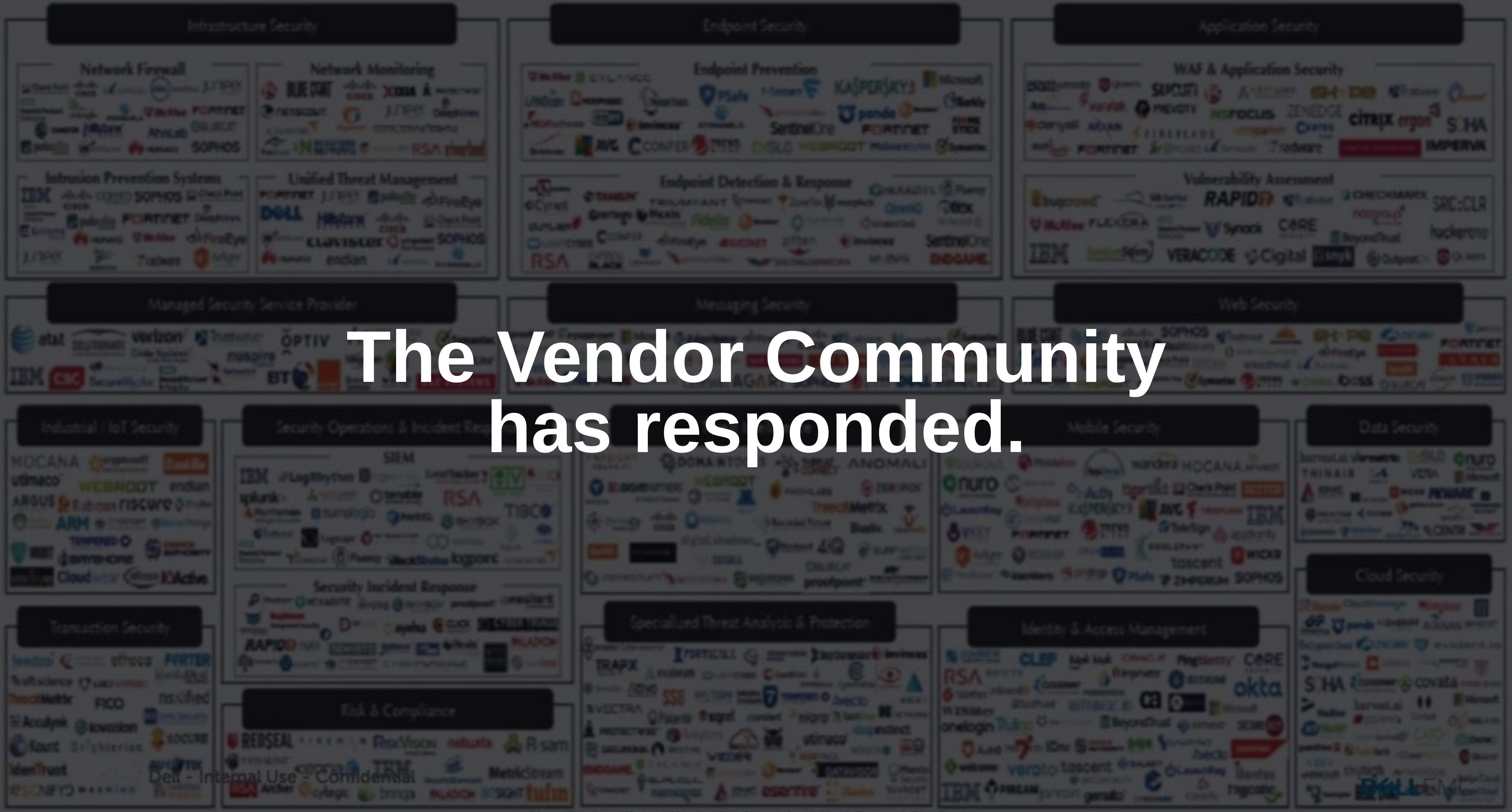
Organizations at Risk

The Tools Shortage

How large is the cybersecurity toolz gap today? According to (IS©)^2 research, the shortage of cybersecurity tools is close to $30 billion globally….



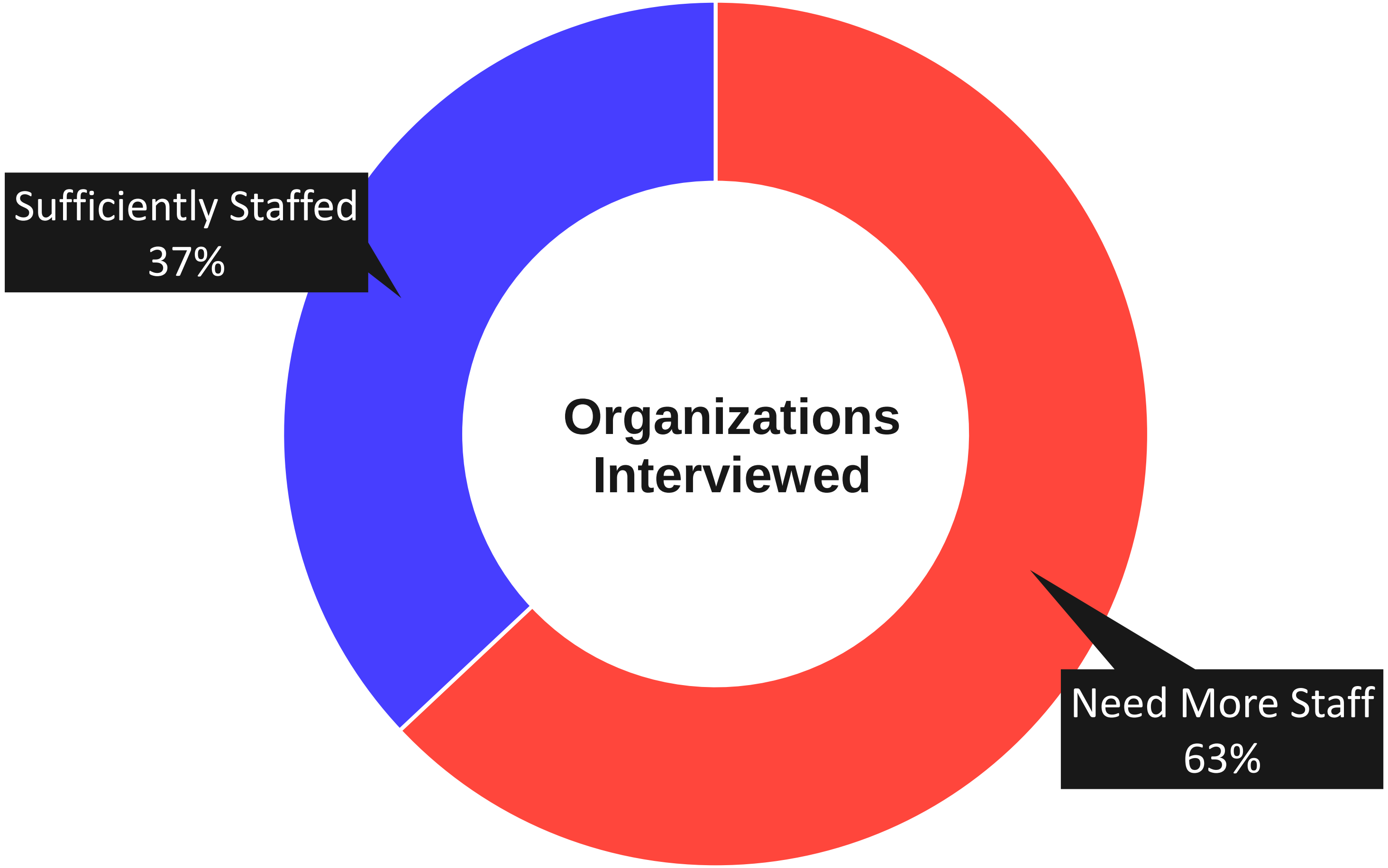
The Vendor Community has responded.

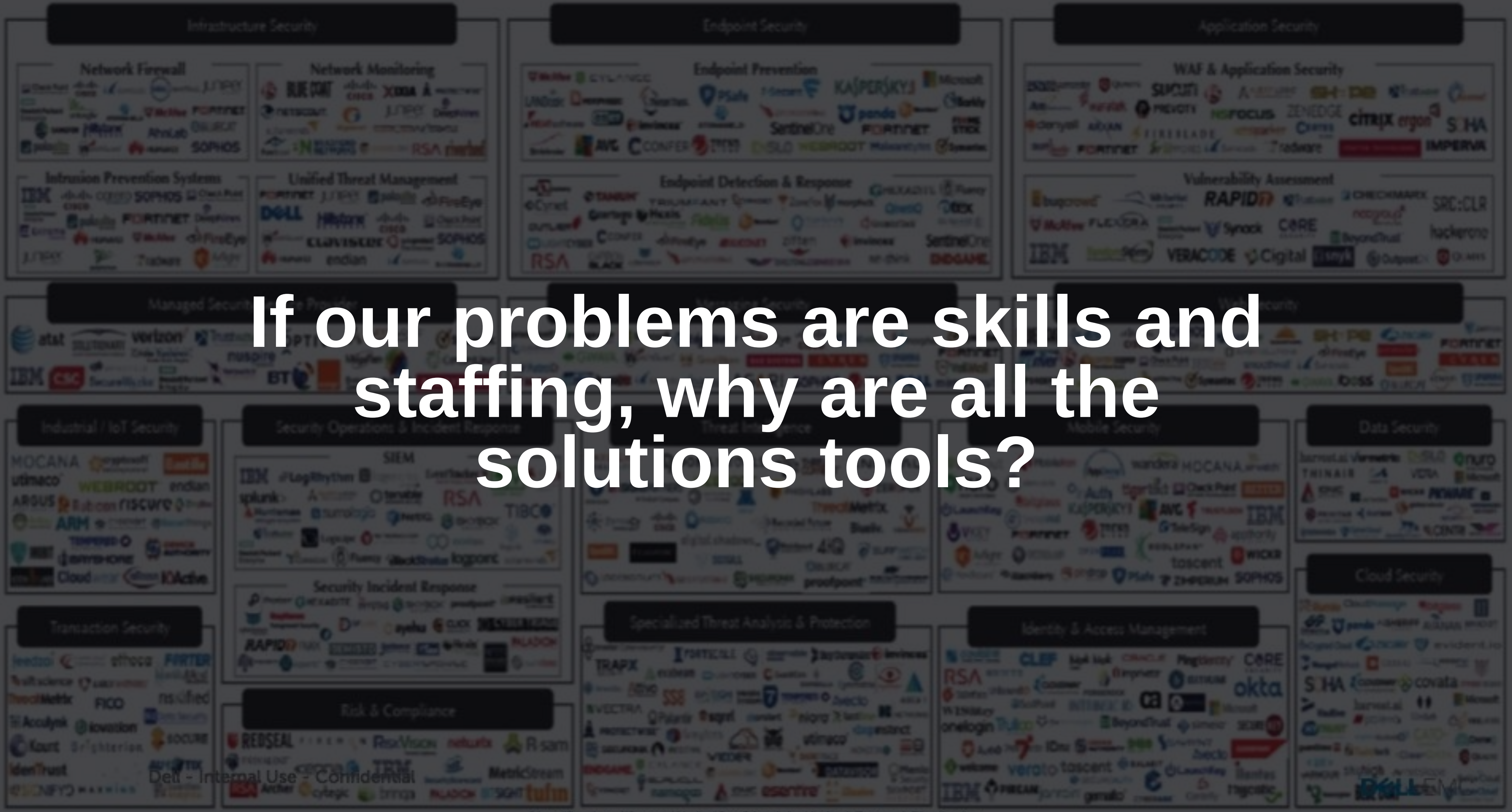

Infrastructure Security
Network Firewall
Network Monitoring
Intrusion Prevention Systems
Unified Threat Management
Endpoint Security
Endpoint Prevention
Endpoint Detection & Response
Application Security
WAF & Application Security
Vulnerability Assessment
Managed Security Service Provider
Messaging Security
Web Security
Industrial / IoT Security
Security Operations & Incident Resp
SIEM
Security Incident Response
Mobile Security
Data Security
Cloud Security
Transaction Security
Risk & Compliance
Specialized Threat Analysis & Protection
Identity & Access Management

Organizations at Risk

The Skills Shortage

How large is the cybersecurity workforce gap today? According to (ISC)² research, the shortage of cybersecurity tools is close to 3 million globally.




Infrastructure Security
Endpoint Security
Application Security
Network Firewall
Network Monitoring
Endpoint Prevention
WAF & Application Security
Intrusion Prevention Systems
Unified Threat Management
Endpoint Detection & Response
Vulnerability Assessment
Managed Security Service Provider
Messaging Security
Web Security
Industrial / IoT Security
Security Operations & Incident Response
Threat Intelligence
Mobile Security
Data Security
SIEM
Security Incident Response
Cloud Security
Transaction Security
Specialized Threat Analysis & Protection
Identity & Access Management
Risk & Compliance

If our problems are skills and staffing, why are all the solutions tools?

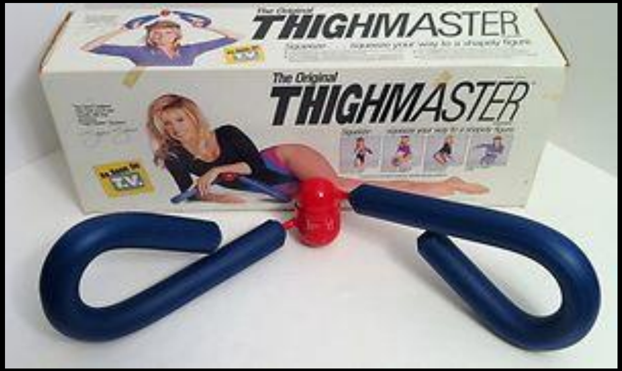
The Bowflex Effect

BOWFLEX
POWER

SHAKE
WEIGHT

The Original
THIGHMASTER
As Seen On T.V.

Measuring Abstract Progress is Hard

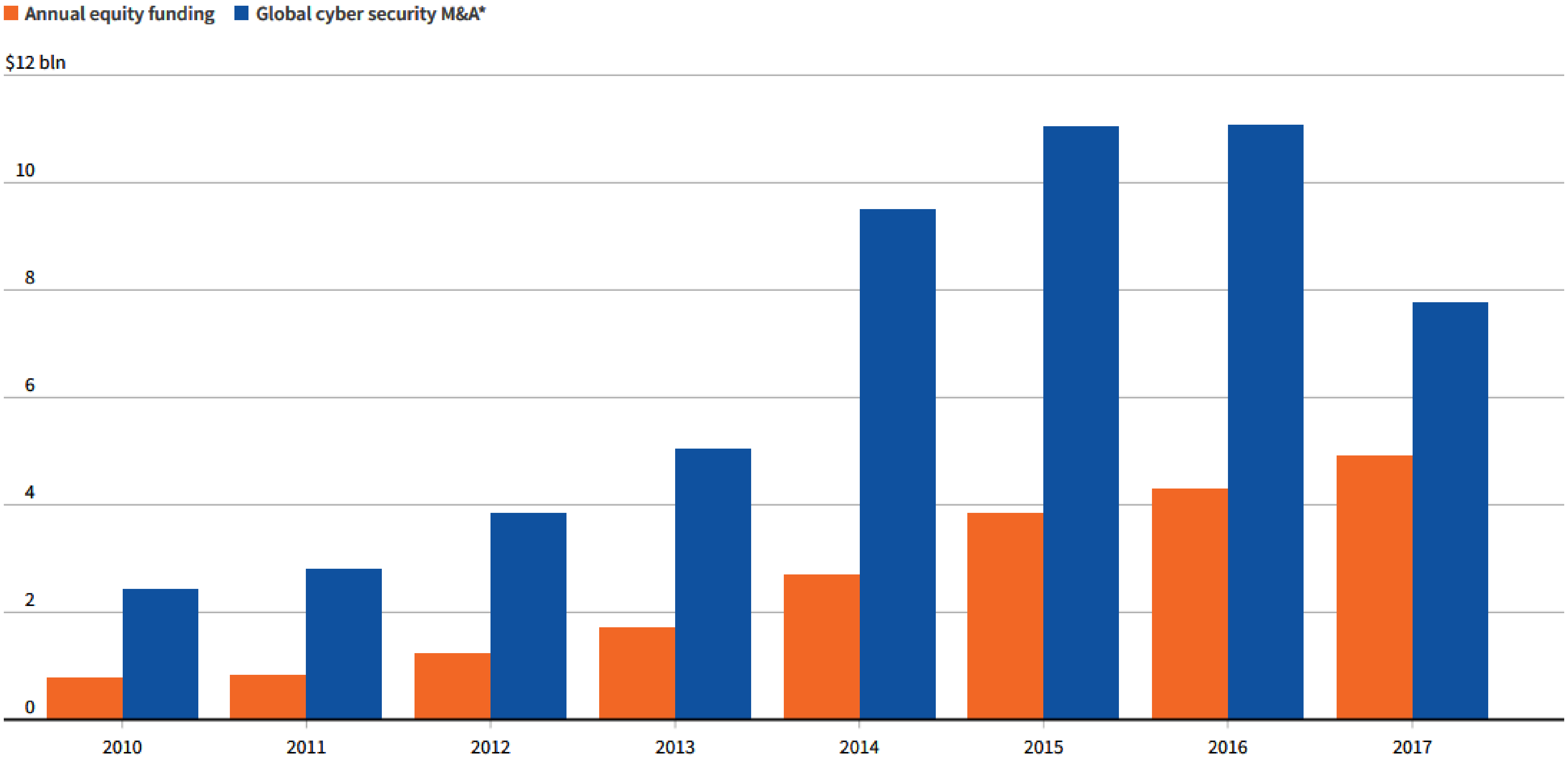
I need to…		How I measure success
…increase lean muscle mass.	→	Bowflex purchased.
…do more cardio.	→	NordicTrack installed.
…tone my thighs.	→	

The Bowflex Effect

Zombie Capital

Zombie capital: Cyber security venture capital funding on the rise while exits fall

Cyber security M&A fell 30 percent last year while VC funding rose 14 percent.

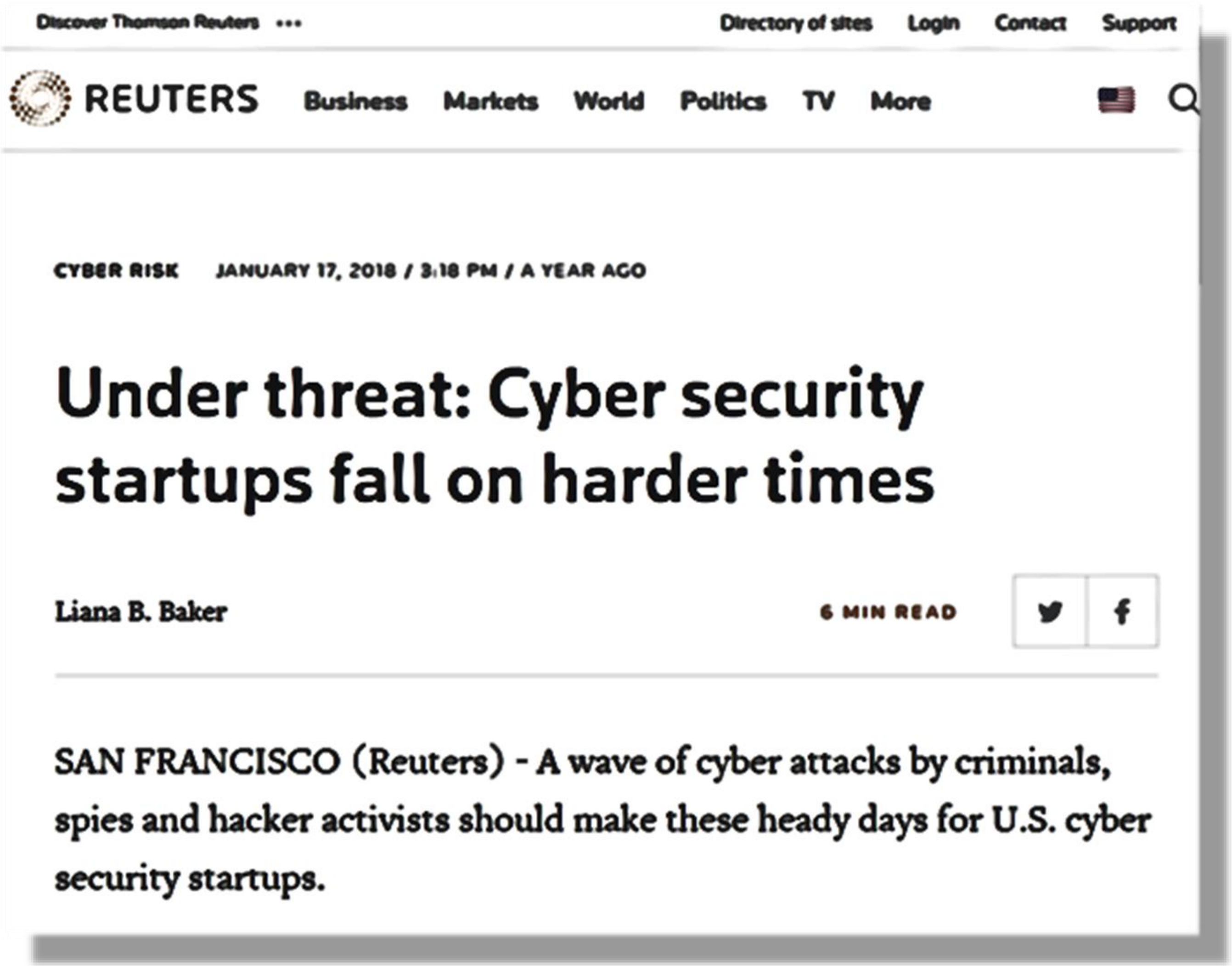


* Where target is privately funded
Sources: Momentum Cyber
Ashlyn Still | REUTERS GRAPHICS

http://fingfx.thomsonreuters.com/gfx/editorcharts/CYBERSECURITY-STARTUPS/0H0010KH07R/index.html

Few of these are pulling off IPOs. What’s more, big software companies have become less willing to acquire cyber security products they believe they can develop on their own.

“Some have compared some cyber security companies to cockroaches,” DeWalt said. “They can’t die, but they aren’t smoking hot either.”



CYBER RISK JANUARY 17, 2018 / 3:18 PM / A YEAR AGO

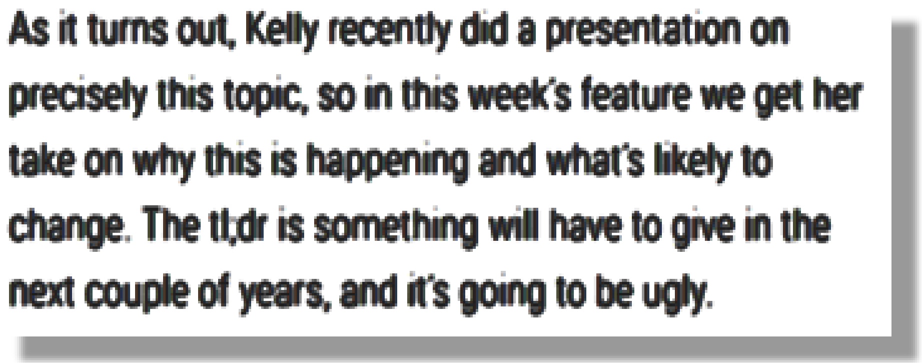
Under threat: Cyber security startups fall on harder times

Liana B. Baker

6 MIN READ

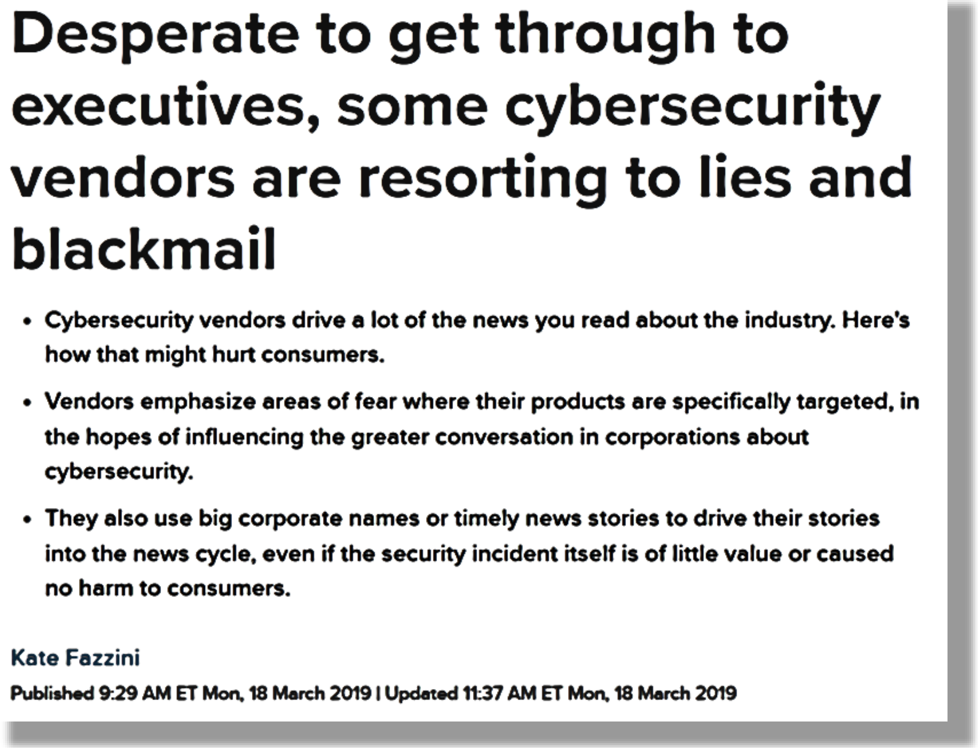
SAN FRANCISCO (Reuters) - A wave of cyber attacks by criminals, spies and hacker activists should make these heady days for U.S. cyber security startups.

https://www.reuters.com/article/us-cybersecurity-startups-analysis/under-threat-cyber-security-startups-fall-on-harder-times-idUSKBN1F62RW



As it turns out, Kelly recently did a presentation on precisely this topic, so in this week's feature we get her take on why this is happening and what's likely to change. The tl;dr is something will have to give in the next couple of years, and it's going to be ugly.

https://risky.biz/RB485/



Desperate to get through to executives, some cybersecurity vendors are resorting to lies and blackmail

- Cybersecurity vendors drive a lot of the news you read about the industry. Here's how that might hurt consumers.
- Vendors emphasize areas of fear where their products are specifically targeted, in the hopes of influencing the greater conversation in corporations about cybersecurity.
- They also use big corporate names or timely news stories to drive their stories into the news cycle, even if the security incident itself is of little value or caused no harm to consumers.

Kate Fazzini

Published 9:29 AM ET Mon, 18 March 2019 | Updated 11:37 AM ET Mon, 18 March 2019

https://www.cnbc.com/2019/03/18/heres-how-cybersecurity-vendors-drive-the-hacking-news-cycle.html

Dr. Quack's
MEDICINAL
~TONIC~
TONIC

EXTRA!
EXTRA!

Process > Tools

Back to Basics

3 Key Processes to Reduce Risk

1. Vulnerability Management
2. Threat Detection
3. Incident Response

Vulnerability Management

22%

Of Incidents SCWX investigated in 2018, the initial intrusion vector was “Scan & Exploit.”

Vulnerability Management

Inspect your current capability.

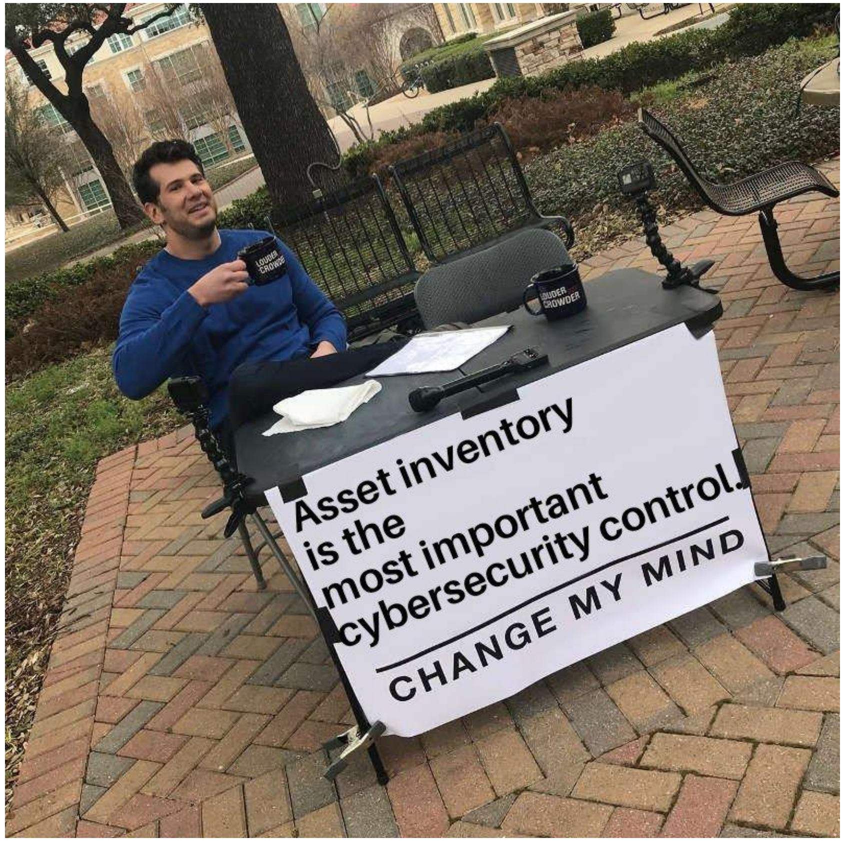
Ask yourself:

- ✓ If a new asset was deployed in my datacenter or cloud, how would I know?
- ✓ How long does it take to deploy updates or configuration changes to my assets?
- ✓ Are my business partners properly managing vulnerabilities of their assets?
- ✓ Which applications are required for my organization to run essential business processes?
- ✓ What evidence do I have to know my environment can resist an attack?

Threat actors, like water, will flow to the path of least-resistance.

Vulnerability Management

Maxims for Success


Asset inventory is the most important cybersecurity control.
CHANGE MY MIND
LOUDER CROWDER
LOUDER CROWDER

Threat Detection

73 days

Average dwell time before an opportunistic threat actor is detected.

Threat Detection

Inspect your current capability.

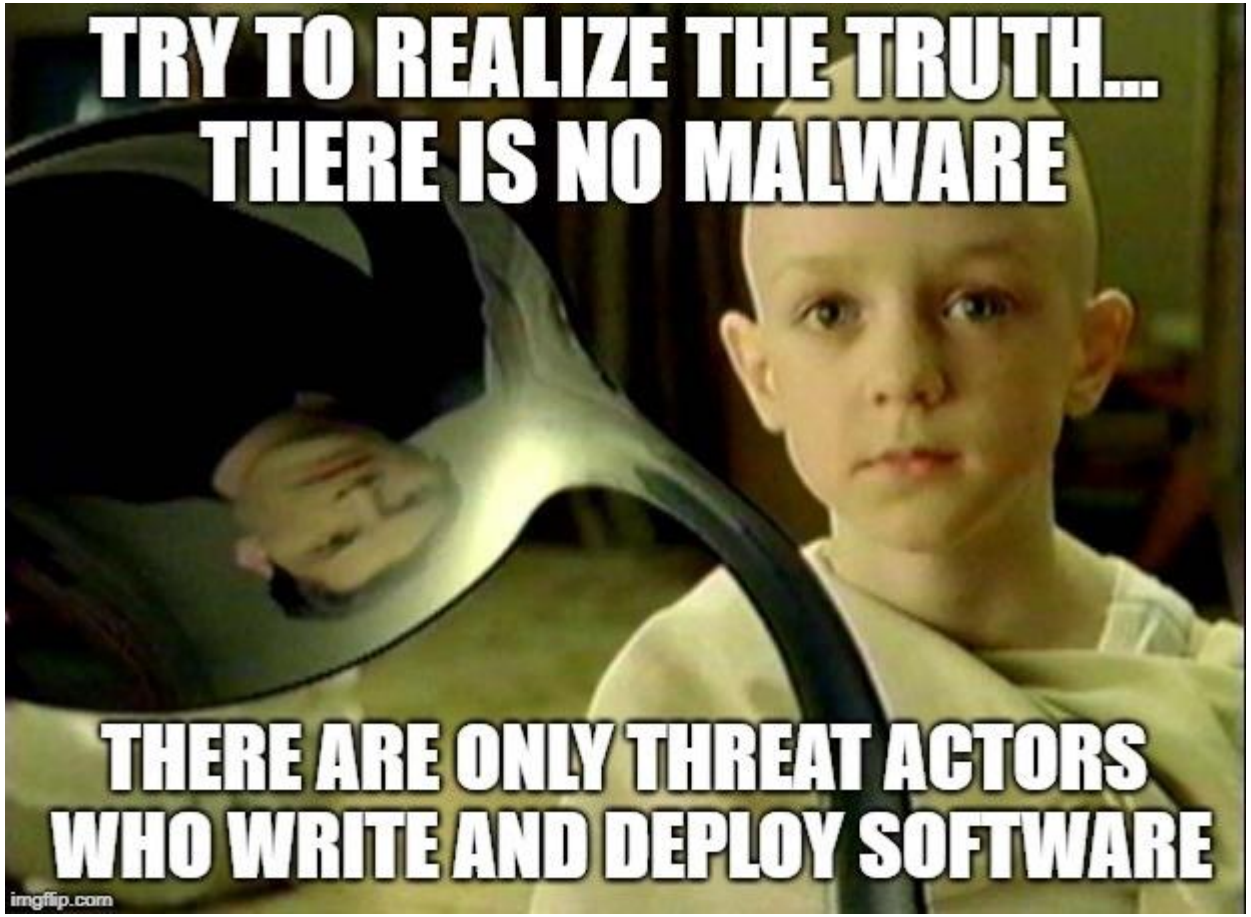
Ask yourself:

- ✓ Do I have the right visibility to detect an attack on our organization?
- ✓ How valuable are my organization's assets to threat actors?
- ✓ Are my security controls tuned to minimize noise and maximize signal?
- ✓ Are threat actors already in my environment? (How would I know?)
- ✓ Are my security controls informed with timely intelligence to detect evolving threat actor techniques?

Threat Actors Will Evade Your Preventative Security Controls.

Threat Detection

Maxims for Success


TRY TO REALIZE THE TRUTH...
THERE IS NO MALWARE
THERE ARE ONLY THREAT ACTORS
WHO WRITE AND DEPLOY SOFTWARE
imgflip.com

Incident Response

85%

of incidents SCWX investigated in 2018 were financially motivated.

Incident Response

Inspect your current capability.

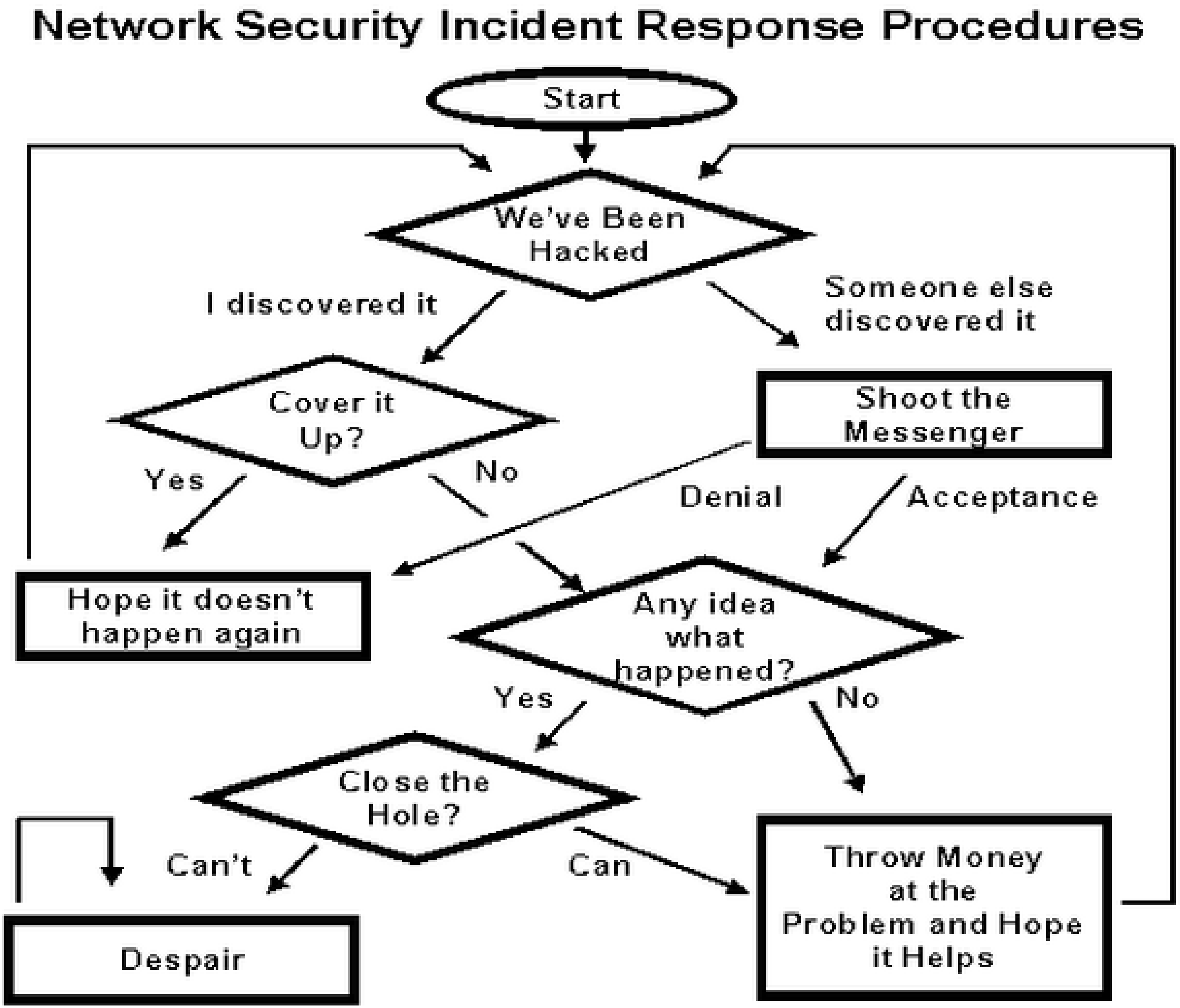
Ask yourself:

- ✓ How many incidents did we investigate last year? What were their severities? How long did it take to resolve each incident?
- ✓ What security controls mitigated the most incidents? What security incidents? What security controls detected the incidents we didn't mitigate?
- ✓ Is the rest of the C-Suite prepared to respond when the inevitable happens?
- ✓ Are my first-responders equipped to respond at 3am?
Does my team have the skills to perform forensics and threat hunting?
- ✓ Do you have an incident response plan? If so, when was it last exercised?

Incidents WILL happen. Is your response capability proportional to the threat, risk, & impact?

Incident Response

Maxims for Success



Network Security Incident Response Procedures

Start

We've Been Hacked

I discovered it

Someone else discovered it

Cover it Up?

Yes

No

Hope it doesn't happen again

Shoot the Messenger

Denial

Acceptance

Any idea what happened?

Yes

No

Close the Hole?

Can't

Can

Despair

Throw Money at the Problem and Hope it Helps

thank you.

Further Reading

Resources and Citations

https://www.secureworks.com/resources/rp-2018-state-of-cybercrime

https://www.secureworks.com/resources/rp-incident-response-insights-report-2018

https://www.secureworks.com/blog/want-better-security-get-back-to-the-basics

https://risky.biz/RB485/

https://www.reuters.com/article/us-cybersecurity-startups-analysis/under-threat-cyber-security-startups-fall-on-harder-times-idUSKBN1F62RW

http://fingfx.thomsonreuters.com/gfx/editorcharts/CYBERSECURITY-STARTUPS/0H0010KH07R/index.html

https://www.isc2.org/Research/Workforce-Study#