




CompTIA.
Partner Summit



The Help Desk, the Security Analyst, and the Kill Chain: A Study in Job Role Morphology

James Stanger, PhD
Chief Technology Evangelist

CompTIA®

August, 2017



James Stanger, PhD

Senior Director, Products - CompTIA

A+, Security+, Network+, MCSE, LPI Linux LPIC-1

Responsible for CompTIA's certifications and continuing education

- *Security analytics*
- *Penetration testing, risk assessment, and intrusion detection*
- *Linux and open source*
- *Network administration*
- *Virtualization*
- *Web technologies*
- *Certification development*
- *Award-winning author and instructor*



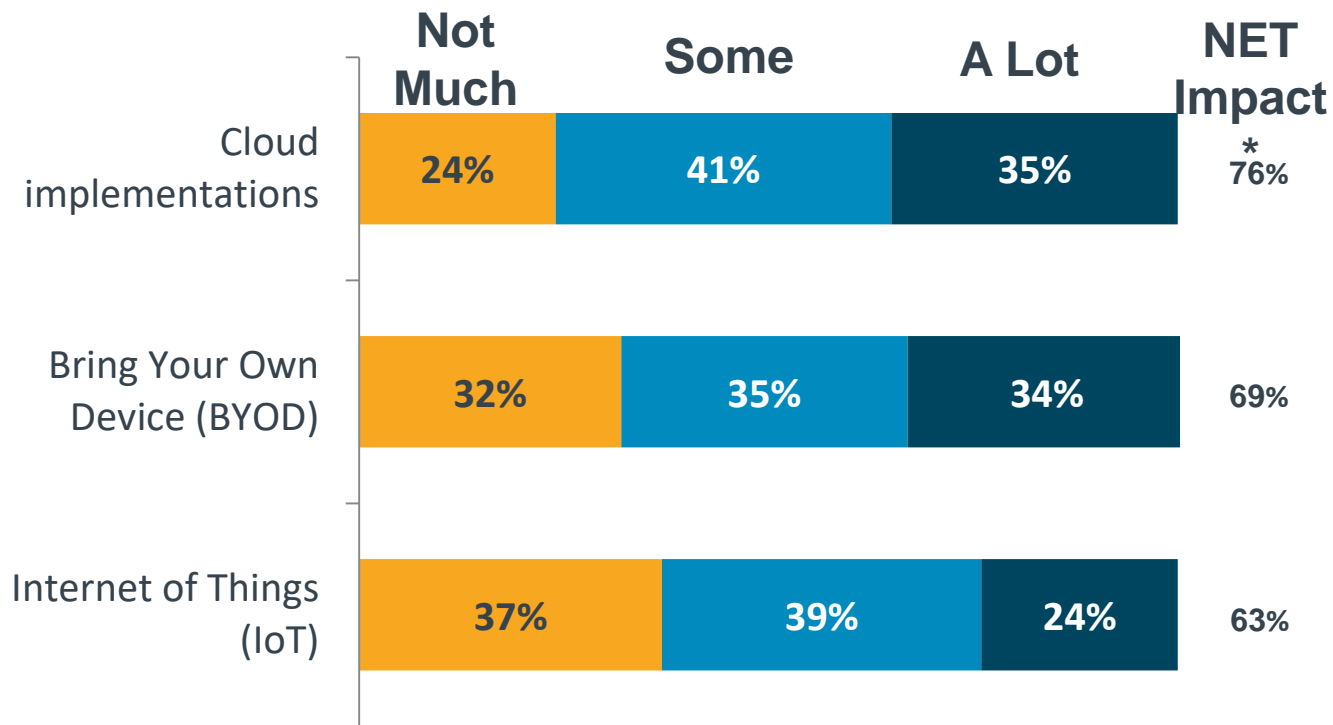
We'll be talking about:

1. A look at how emerging tech and the latest types of attacks exploit the business environment
2. How changes in cybersecurity have impacted the practical role of the ITSM professional
3. The steps to take when managing typical behaviors during a security incident

Over the past few years, we've heard sad (and sometimes tall) tales about devastating Distributed Denial of Service (DDoS), zero day, vendor impersonation, and social engineering attacks. Attacks seem to continue unabated. But some things are, in fact, changing. Join Dr. James Stanger to learn more about CompTIA's research into critical job roles and responsibilities in today's organizations. Using CompTIA research gathered from IT pros around the world, he'll discuss how industry response to attacks over the last few years has helped morph key job roles in the industry. For example, research is showing key shifts in the security analyst and help desk job technician roles. After this presentation, you'll have greater insight into how the Information Technology Service Management (ITSM) community fits into the security kill chain

**emerging tech, and the latest
attacks exploiting our business
environment(s)**

Emerging tech impact on security issues at the help desk

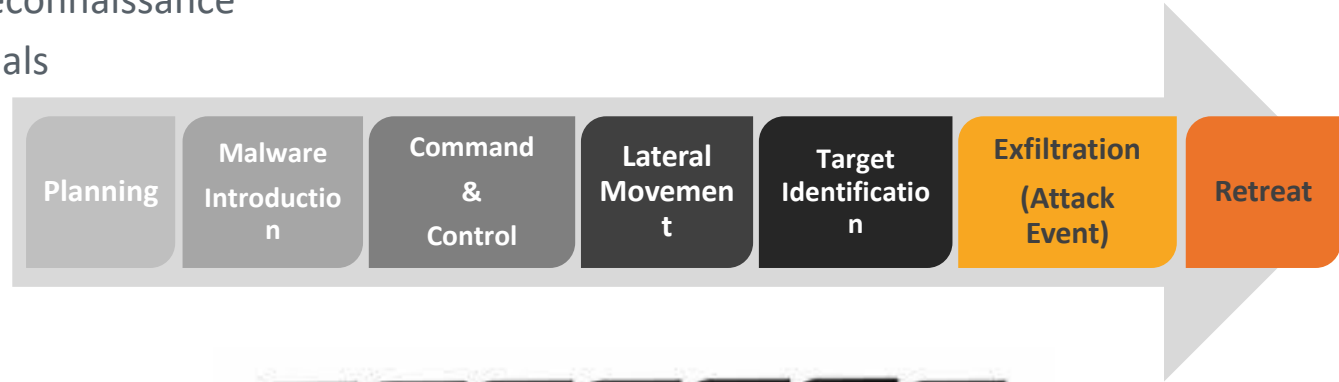


*NET Impact: Some + A Lot

The Advanced Persistent Threat (APT)

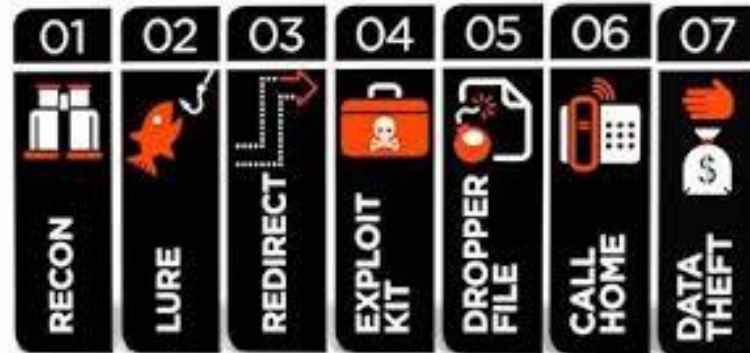
- Long-term infiltration

- Requires significant reconnaissance
- Highly-skilled individuals
- Traditionally state-sponsored
- Not as much anymore



- Help desk issues

- Weak authentication
- End points
- Practical monitoring
- IP theft issues
- Covert channels



Ransomware

- One of the biggest issues today
 - How it gets in
 - What it can do to a company
 - Where is the help desk in all of this?
- How to address it
 - Training
 - Removal / payment
 - Creating a resilient presence



“It’s a 1-billion dollar a year business that is now in the cloud.”
-- John Dvorak, formerly of the United States Federal Bureau of Investigation (FBI)

“Our organization has been the target of multiple phishing attacks in the past year. We have utilized our helpdesk to communicate with end-users and provide user education regarding how to spot and avoid phishing scams.”

Hacking as a service (HaaS)?

Just outsource for your hacking needs:

- No need to even be technical
- Physical attacks
- Warehousing stolen data and criminal data
- Hacktivism
- Attacks originate from inside and outside the company

Recent prices from the black market

1BTC
213,200 EUR

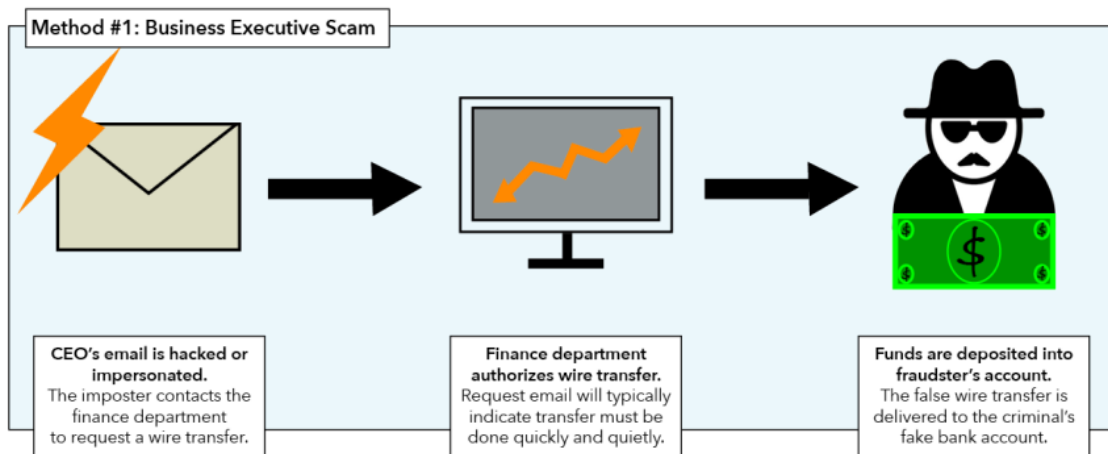
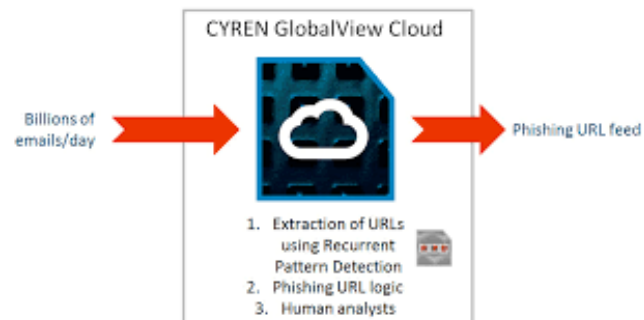
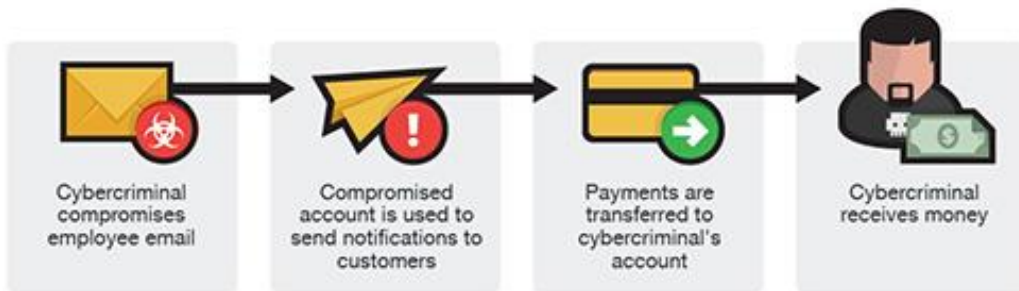
N	SERVICES	BTC	EUR
50.000	Root shell	1,85	394,62
45.000	Wordpress admin passwords	1,50	319,80
50.000	SSH sniffer logs	1,20	255,84
1.000	Linux botnet	2,00	426,40
1.103.504	FTP/SSH passwords	3,00	639,60

N	SERVICES	BTC	EUR
1	Start your own market	33,48	7.137,00
1	Virtual credit card + bank account	0,01	2,69
1	Unlimited REAL code signing	4,20	895,44

TYPE	KIT	BTC	EUR
spam	Wordpress Comment Spammer + Exploit	2,50	533,00
malware	Bitcoin Ransomware	0,21	44,77
malware	Tomcat Worm	7,40	1.578,67
malware	The real GovRAT	4,50	959,40

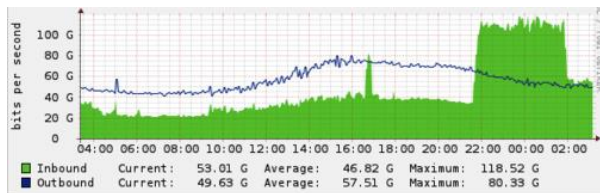
TYPE	EXPLOIT	BTC	EUR
1day	MS15-034 Microsoft IIS Remote Code Execution	308,53	65.778,11
1day	*NEW* ring0 LPE Exploit CVE-2015-0057	48,17	10.269,84
fud	Adobe Flash < 16.0.0.296 (CVE-2015-0313)	2,50	533,00
Oday	Internet Explorer <= 11	35,00	7.462,00
Oday	Android WebView Oday RCE	36,50	7.781,80
Oday	Linux <= 3.13.0-48 Kernel Panic	2,00	426,40

Business E-mail Compromise (BEC) and the cloud



DDoS attacks – the old is new again!

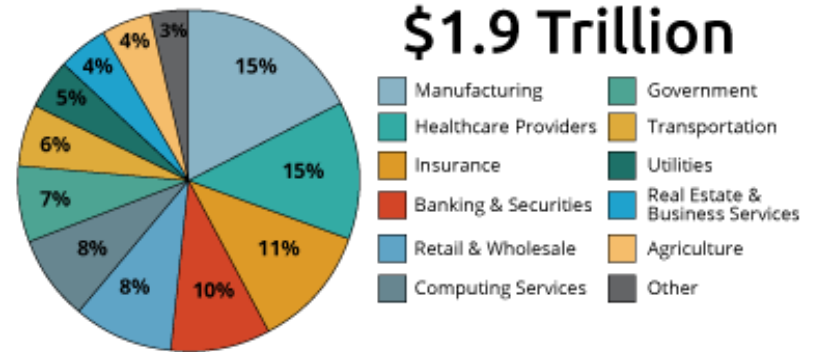
- Major attacks in the news
- Characteristics
 - Can last for hours
 - From botnets
- IoT and DDoS
- The cloud – tenancy



The Internet of Things (IoT) – a buzz-phrase that still works

- Some definition(s)
 - “A global system of interconnected computer networks, sensors, actuators, and devices”
 - Machine-to-machine interaction
 - From network-enabled devices to network-enabled lives
 - Wearable tech
 - Smart cities
 - “Internet of Everything”
- 24,000,000,000 connected devices by 2020 – *and 12 billion of those will be mobile*
- Terms
 - Sensors, context awareness, and analytics
 - In-memory computing
 - Mobile workforce – *and at play, too*
 - Analytics
 - Data volume

Internet of Things Value Add by 2020



Kevin Ashton coined the term “IoT” back in 1999

Practical IoT – four major technical perspectives

1. Development of the IoT device
 - Firmware / storage
 - Connectivity
2. Network creation – making it work
3. Maintenance – keeping it working
4. Data analytics
 - Crunching numbers
 - Identifying trends
 - Determining product placement
 - Product features
 - New data streams



Considerations: Speed to market, ease of communication, ability to *monetize*. Security considerations? Meh – secondary at best!

What IoT became last October

- The Dyn attack heat map, October 2016
- Just an example of what can – and will – happen worldwide

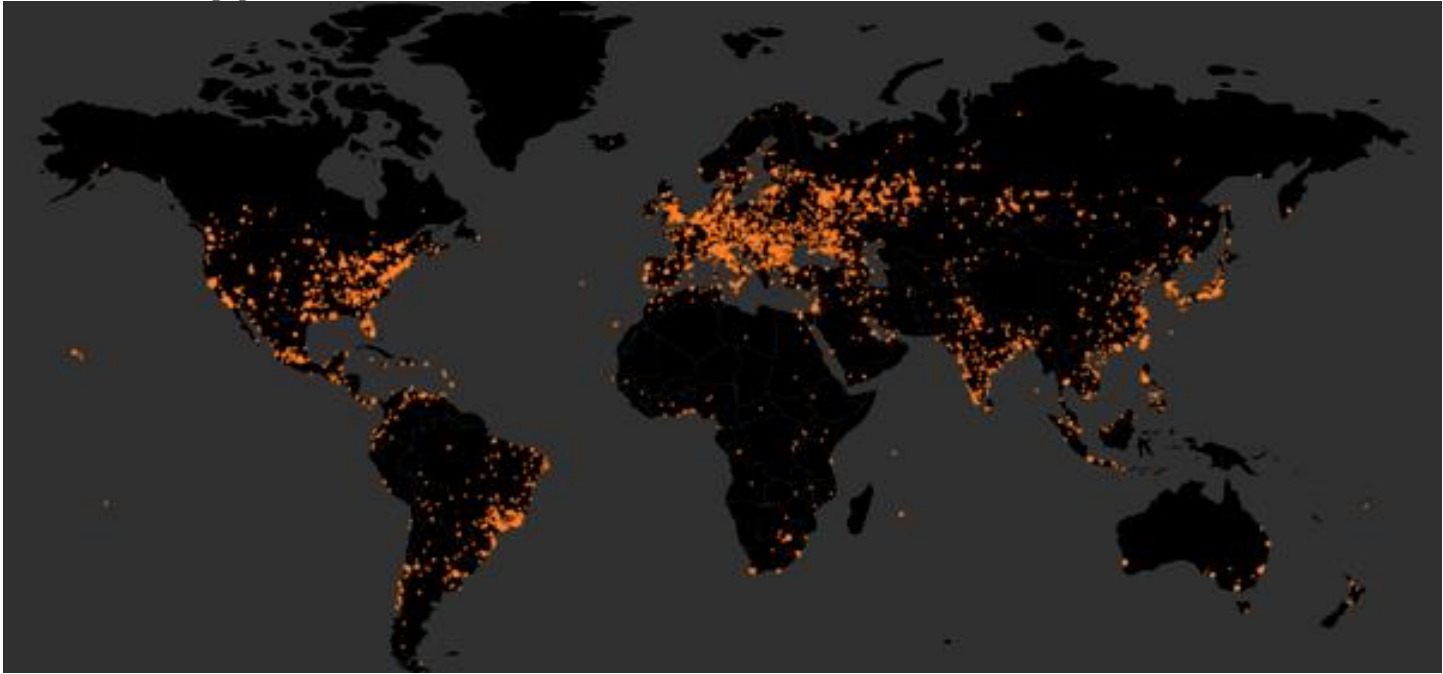


*The question:
What was the
real object of
this attack?*

*Also: The
WannaCry
attack of 2017*

Another heat map – just last month

- Wannacry – one company's take on the most-hit areas of the world



What does this all have to do with the help desk?

- In some ways, *nothing*.
- In a very important way: *Everything*

Disturbing trends

Leaving IT security to “someone else”

- The “security team”
- Ignoring key teams, including the help desk

Working in isolation; security silos

- Once an attack begins, response is left to only one part of the team
- Improper communication
- “Tickbox” approach to security
- Plenty of data is created
- But little information is created or acted upon
- The lack of information includes ignoring the help desk
- The result? Lower net security



Trend: Help Desk supports more business units than ever before; there is potential for the help desk / service tech to break down silos

A conundrum – and, the stakes are high

- More resources are being directed at security than ever before
- Yet, attacks are on the increase
- They're also getting more severe
- Why is this happening?
- What approaches will help reverse this trend?

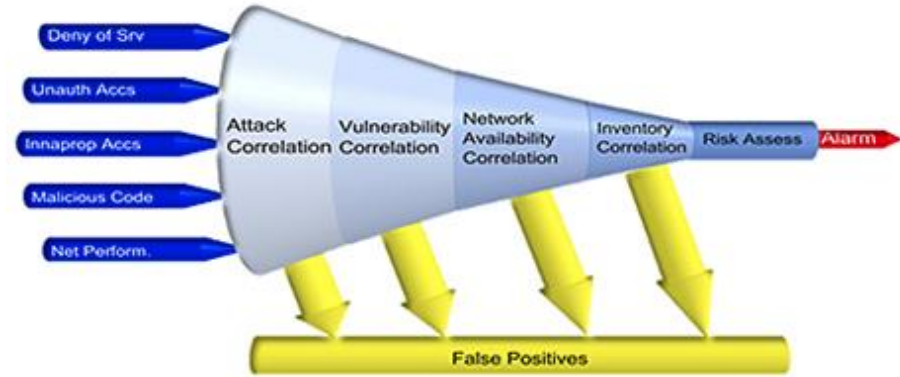
It seems that we're leaving out a critical part of a company's response to security threats today – the help desk

Gartner: Over \$75 billion spent in 2015 alone. Over \$300 billion lost.

According to the Ponemon Institute, over the last five years, 2,800 publicly disclosed data breaches occurred to the tune of roughly \$139 billion.

The security analyst job role is born

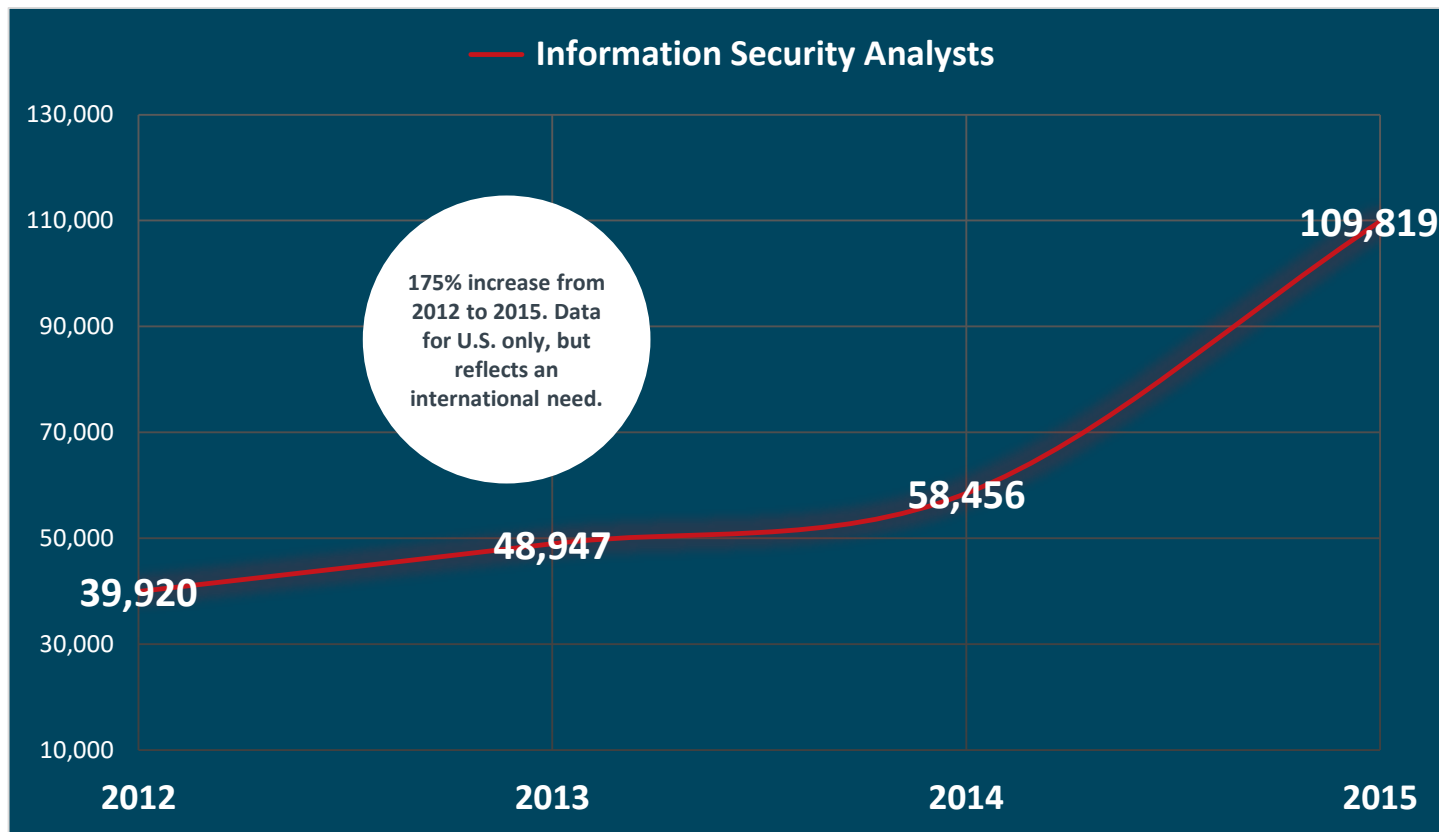
- Apply “big data,” behavioral analytics, and dashboard-based visualization to the IT security market to improve the overall state of IT security.
- Focus on network behavior in an organization’s interior network
- Identify network anomalies that indicate bad behavior



Security analyst skills include:

- ✓ Threat management
- ✓ Vulnerability management
- ✓ Cyber incident response
- ✓ Security and architecture tool sets

Security Analyst Job Role – number of job postings

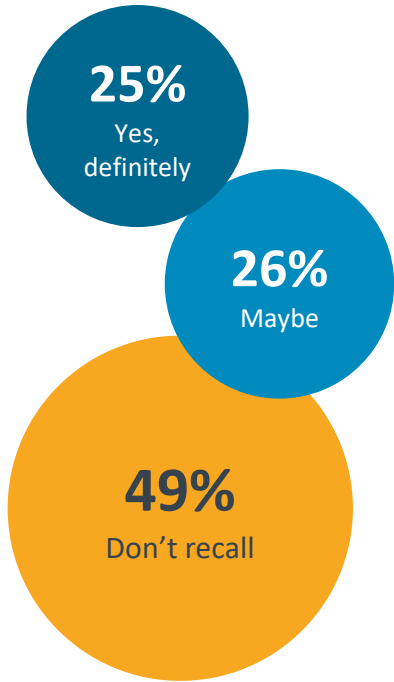


**So, what is this “kill chain,”
anyway?**

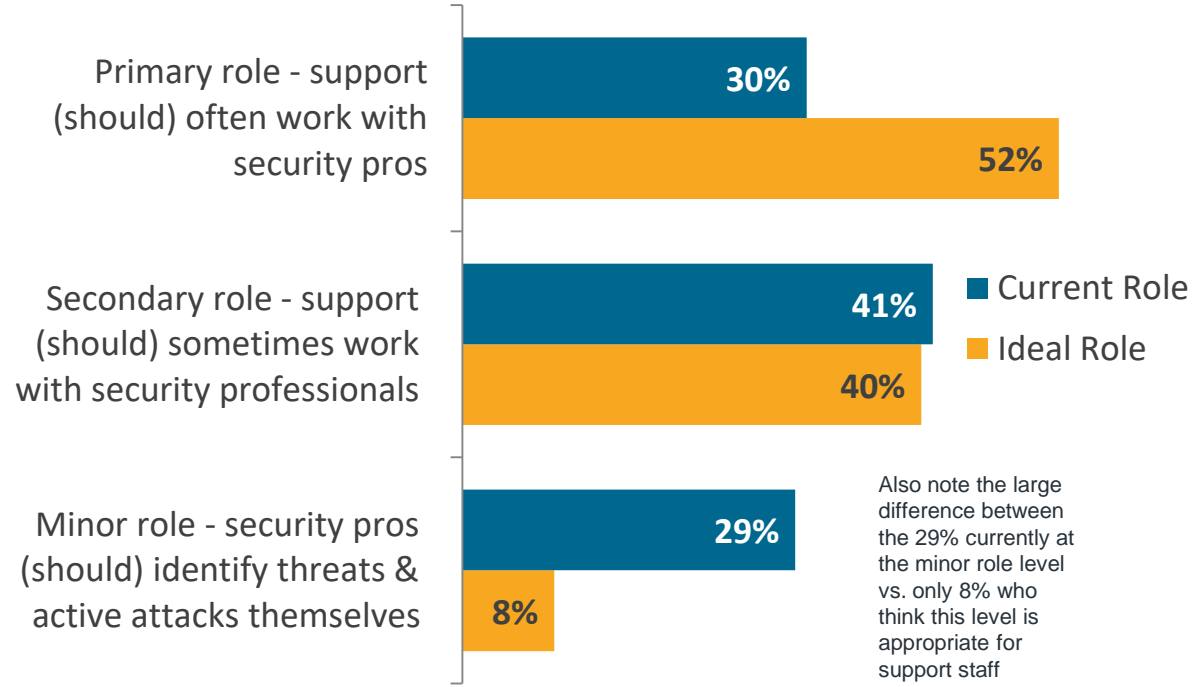
The “kill chain” concept

About one-half of IT pros recall seeing or hearing about the concept of the “kill chain” in regards to security. Regardless of awareness, over half believe support should play a primary role in the kill chain (52%), but it’s currently a primary role for only 3 in 10 (30%).

Awareness of “Kill Chain” Concept



IT Support’s Current Role vs. What it Should Be in the “Kill Chain”



Source: CompTIA IT Security and Support | Overall results, n=439 IT pros

Background about the “kill chain” concept

- Model for attacks developed by Lockheed Martin practitioners in 2010

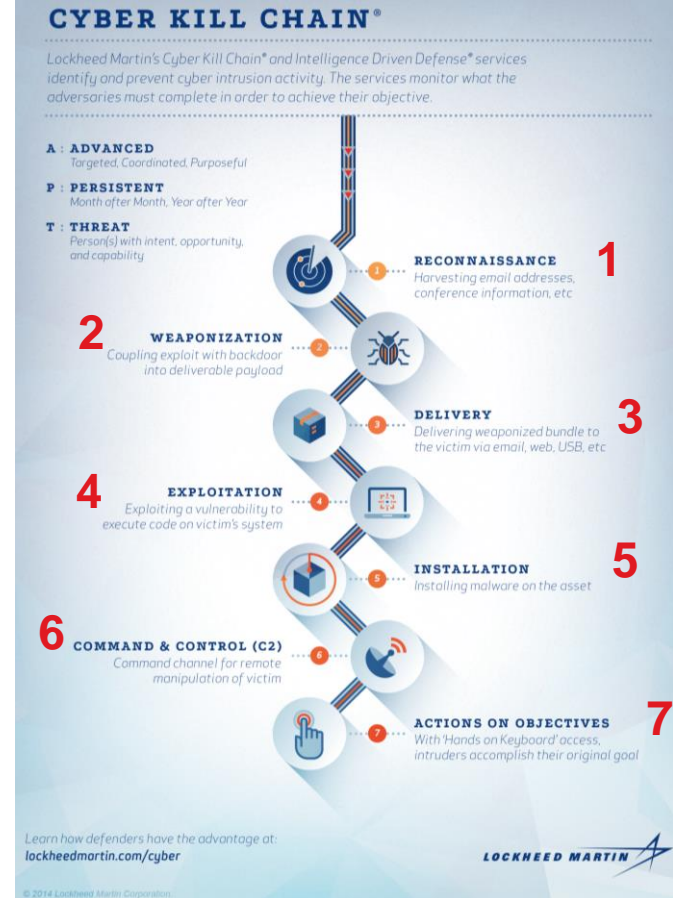
Essential question: What is the role of the help desk in each of these steps?

- A borrowed military concept

- Is it still a valid model?

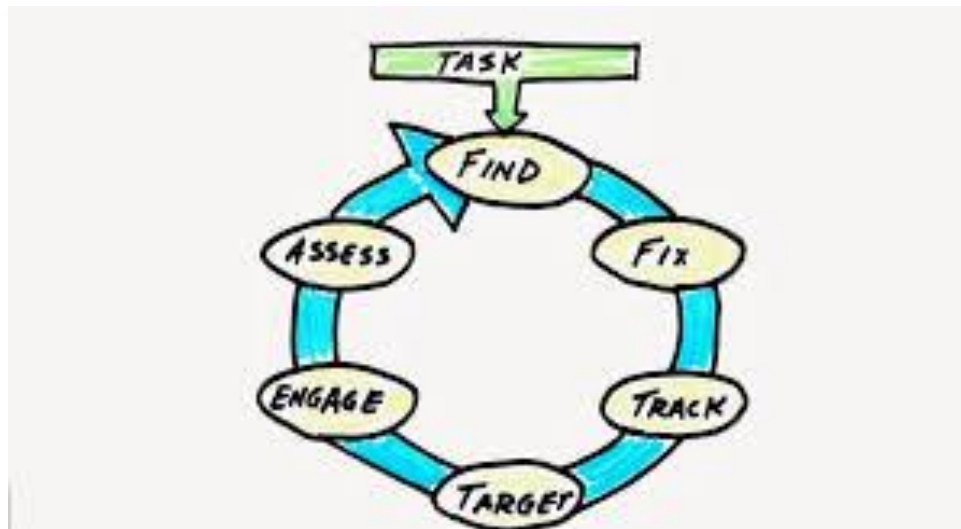
- Perimeter-focused
- What about the cloud and IoT?
- What about the APT?
- A systems focus, not on end users

URL: <http://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html>



Why did they think of the “kill chain?”

- They started crunching the numbers
- They could affect the behavior of roughly 10% of their end users through training
- Numbers:
 - 126,000 employees
 - 10%: 12,600
 - Multiply this by the number of open ports (65,535): 825,741,000
- So, they started thinking about how to manage the chain

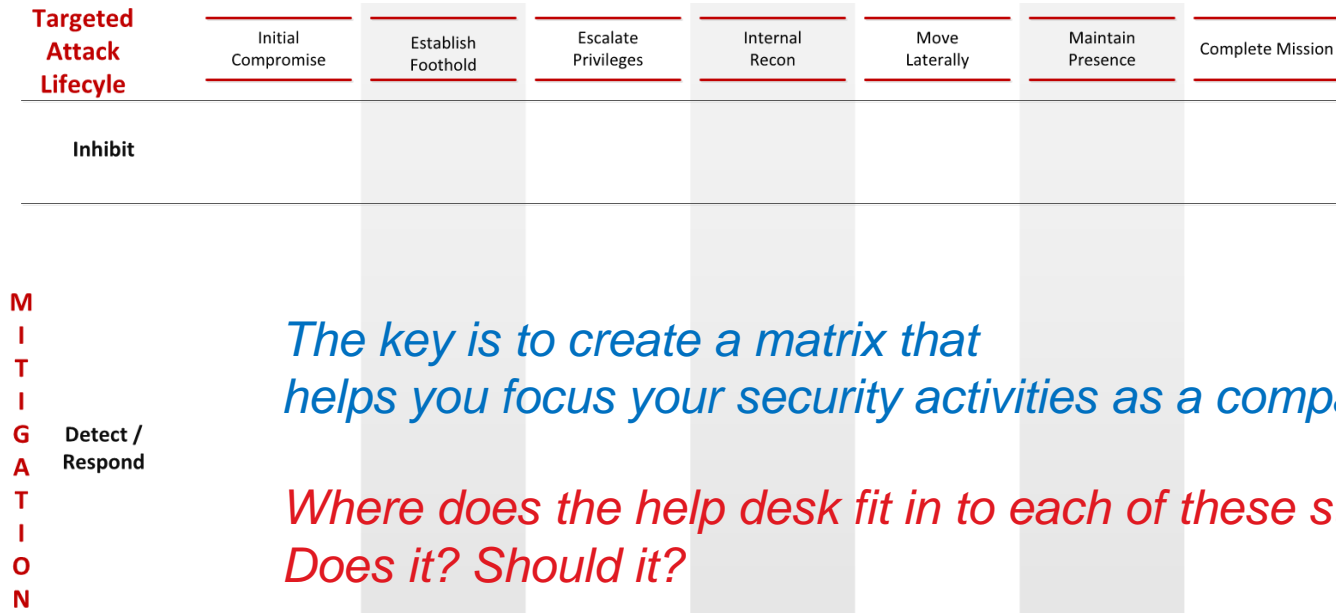


“f2t2ea”

The Lockheed Martin employees:
Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin

The kill chain and frameworks

- It's vital to focus on identifying the hacker cycle
- Mitigation involves inhibiting the hacker as well as detection and response



thoughts from an executive concerning the help desk and security

Thoughts from an exec in the field . . .

“I think they could absolutely be an important component in a mature organization. The biggest inhibitor of your thinking is that **most organizations I’ve looked at don’t do data analysis on their tickets for patterns which would indicate a problem.**”

Without data analytics across the tickets you’ll only spot an issue if there are either enough issues for a single help desk person to spot the pattern as most help desk operations are run with KPI’s like how quickly tickets are resolved which tends to inhibit the behavior of deeper analysis and pattern finding. But **I completely concur that with proper process building and training for the help desk staff they could be a very solid “early warning” vector of a range of security issues.**”

-- Sr Director Security Architecture & Engineering
Major US retailer (online and brick and mortar)

More thoughts . . .

“Interestingly to my perspective is that security also can affect help desk volumes directly. I discovered this in a previous organization where we, for want of a better word, declared war on malware. We had had some very sensitive data exposed by malware which resulted in the executive leadership wanting us to find and destroy all malware of any type. **After about six months of using a bunch of techniques to find and eliminate all malware (including stuff like potentially unwanted software) the volume of help desk tickets at that organization reduced by nearly 60% and there was a clear causal relationship. We discovered when we dug deeper that all sorts of problems like “printer” issues were in many cases a symptom of a host having malware of some sort on them.**

So bottom line is I think there is **a lot of untapped synergy** between help desk and security where both groups could help each other.”

-- Sr Director Security Architecture & Engineering
Major US retailer (online and brick and mortar)

The service desk and the “fog of more”

- A phrase coined by Tony Sager, formerly of the NSA
- Too many tools around
- Too much information
 - One reason behind so many attacks today
 - Serious cost issues worldwide – auditing
- The help desk worker can help provide clarity



Help desk / service desk input for the security team

Table 1. Kill Stages of an Advanced Attack

Attack Stage	Malicious Action	Kill Steps
Reconnaissance and Weaponization	<p>After some initial public information lookups, the attacker scans the network and finds a vulnerable DNS server.</p> <p>The attacker modifies his toolkit to exploit the vulnerability and load botware onto the DNS server, use the DNS traffic to hide its command and control activity and be able to move bots around to other DNS servers as needed.</p>	<p>This is a difficult point at which to create a kill action; however, preventive actions here could go a long way. Inventory of applications and versions, patching and awareness of the patch level would protect against discovery of exploitable vulnerabilities.</p> <p><i>The best “kill” action can take place at the help desk!</i></p>
Delivery	<p>The attacker uses a vulnerable UDP port to load the malware, then establishes the communication channel with the master controller.</p> <p><i>Problems with accessing sites – routing issues or APT?</i></p>	<p>Intelligence applied with DNS monitoring at this layer would watch for unusual UDP/TCP traffic, along with URL filtering and comparison to known command and control signatures.</p> <p>If this is a new exploit, protections must be built on the fly to prevent breach while the UDP vulnerability is under repair. That prevention information should be shared with the larger community of users and vendors for the protection of other legitimate businesses that could be victimized by such an attack.</p>
Install and Spread	<p>The DNS server is set up as a launching point for finding hosts that can be infected inside the organization.</p>	<p>Unusual traffic between servers that usually don’t talk to one another is another behavior that intelligent sensors should be able to detect, examine and block.</p>
Establish Command and Control	<p>Once established, inbound commands are sent to the exploited DNS server, which returns outbound traffic and/or begins identifying other vulnerable devices within the organization to exploit.</p> <p><i>Help desk and reports concerning problems with slow server/service</i></p>	<p>All of these actions create changes to the system that show up in logs and traffic reports.</p> <p>Intelligent tools should pick up and report on unusual connections between servers and devices, to-from locations, types of traffic and the ports used. If connections are suspect, tools should capture traffic between the servers for further examination, including decrypting packets and examining contents, when required.</p> <p>Watching for patterns of repeated downloads, uploads or lateral movement of files is one way to detect and kill the attack before sensitive data gets out.</p>
Task Accomplished: Data Exfiltration	<p>The attacker has control of the target systems and is sending data outside the organization.</p>	<p>Outbound traffic monitoring can catch this last stage of attack. However, criminals have learned to send their data from unsuspecting servers and use low and slow bursts to try and thwart outbound protections. Advanced tools should make determinations on outbound traffic based on traffic type, to-from pathways and other patterns to detect sensitive outbound data in egress traffic.</p>

The kill chain and the help desk

Kill chain step	Description	Help desk role
Reconnaissance	Attack patterns, threat landscapes, scans	Social engineering detection, traffic identification
Weaponization	Coupling remote access with an exploit	Noticing where things fall in “cracks” between systems. Knowing business value of systems
Delivery	Transmission of the weapon to the target. Software installation, compromise, process management	Applications being installed. Monitoring of processes. End user complaints concerning apps and OS.
Exploitation	Triggering of the code to conduct the exploit	Alerts, either by end users or software or security professionals.
Installation	Code runs persistently	Identifying application behavior. New applications present on the system.
Command and control	Traffic dedicated to managing installed code	Systems behaving abnormally; slowdowns.
Actions on objective	Involves exfiltration of data. Involves data integrity issues, lateral movement.	Files deleted or added. New software. Open ports.

Creating a dynamic defense

- Focus on being proactive, not reactive
 - Custom detection tied to actors
- Detection across attacker lifecycles
- Analysis and intel-driven
- Self-notifying
- Resilience
 - Coordinated
 - Anticipatory
 - Responsive & Agile
 - Externally sharing

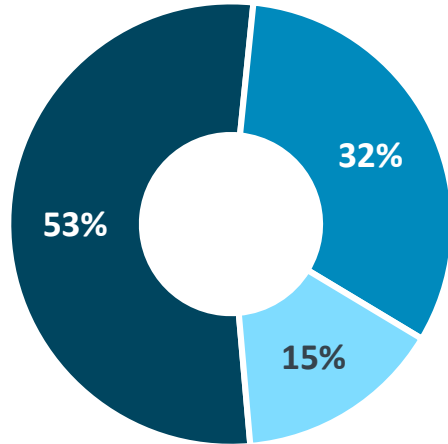


The help desk becomes a major part of an integrated through resilient approach.

Current perceptions about the role of the help desk / service desk professional

Role of IT security at the tech support / help desk level

Slightly over half indicate that security is a primary responsibility of the support function (53%), while it's more of a secondary responsibility for nearly one-third (32%).

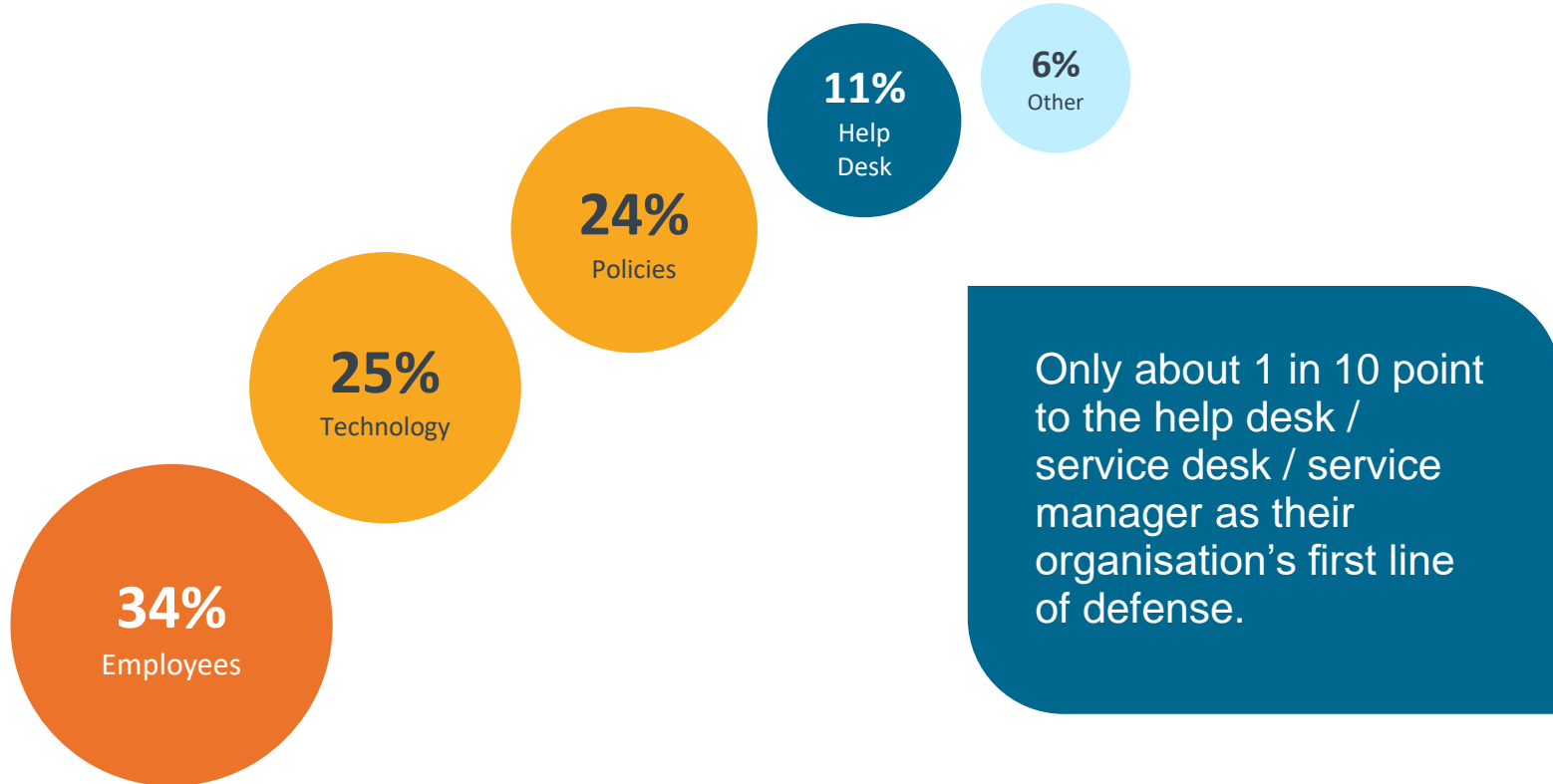


- Security is a primary responsibility of support
- Security is a secondary responsibility of support

Security is a primary or secondary responsibility for NET 85% of companies.

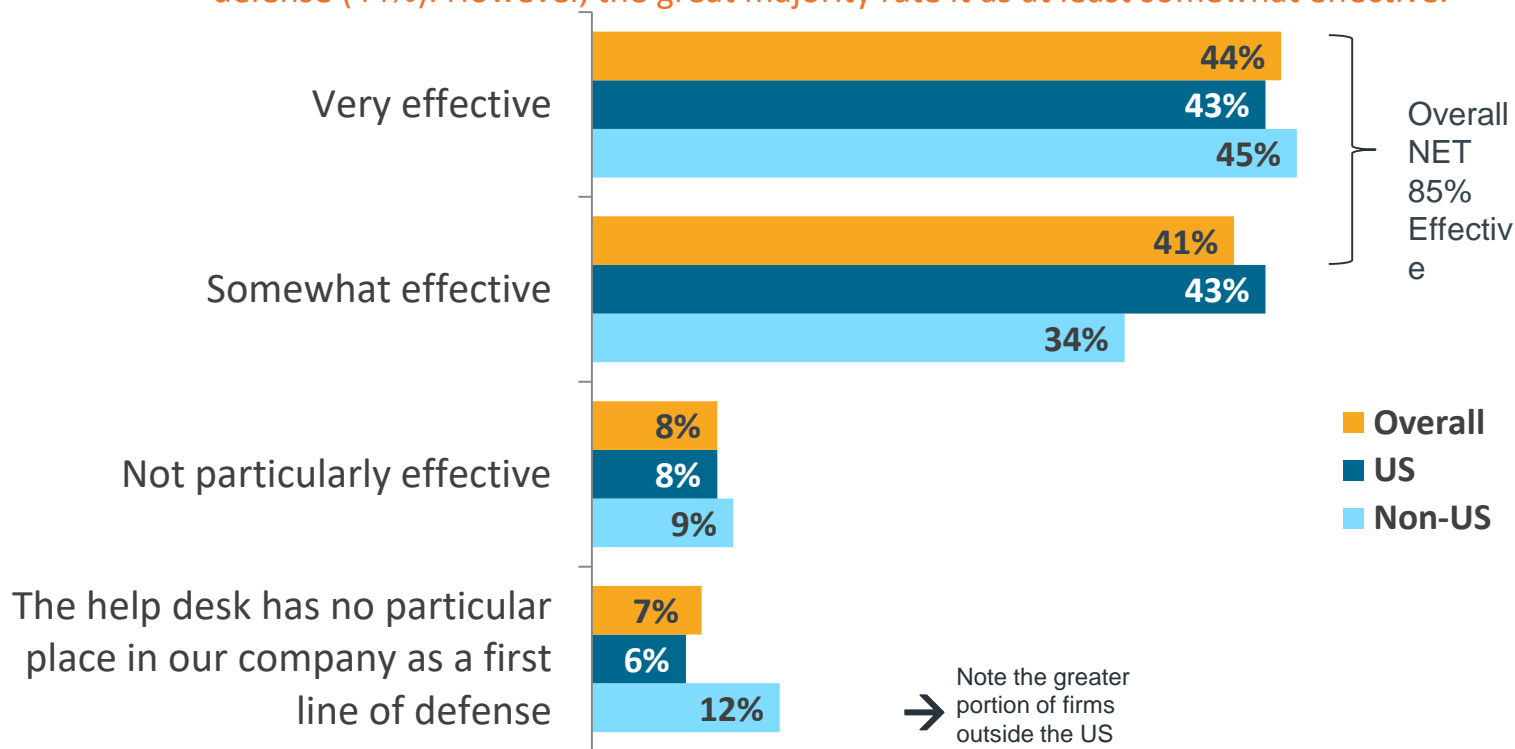
Who or what is the first line of defense?

Approximately one-third consider employees in general to be their company's typical "first line of defense" in regards to IT security (34%).

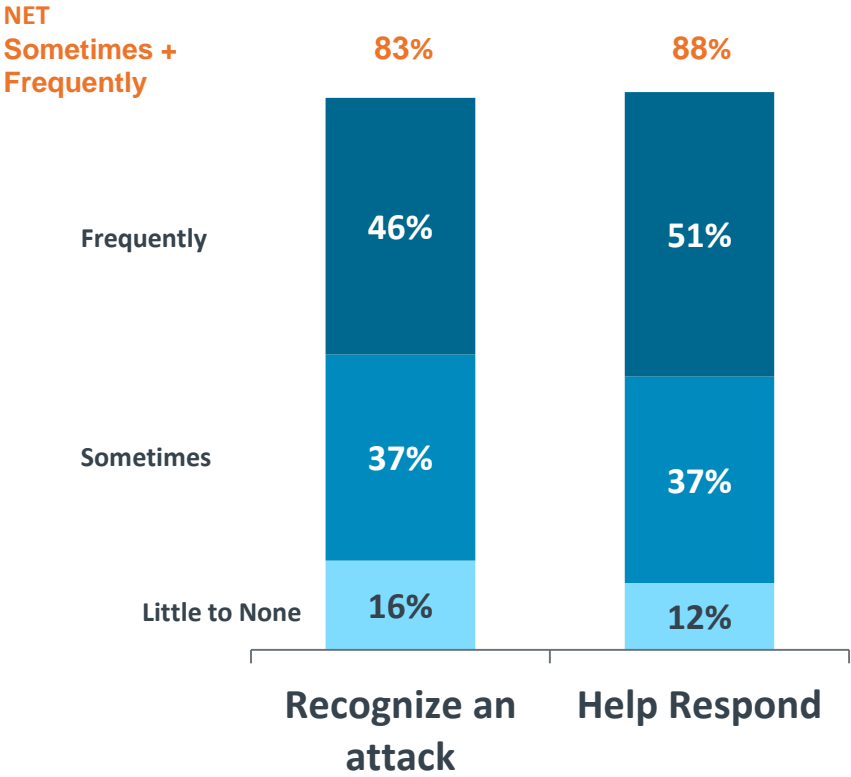


Effectiveness of support as the first line of defense

Less than half rate their firm's help desk as being a very effective first line of defense (44%). However, the great majority rate it as at least somewhat effective.



Frequency of support workers recognizing and responding to attacks



About half report their company's support / help desk / service workers *often* being able to recognize an attack or help in its response.

Furthermore, the great majority indicate support staff is at least sometimes involved in these actions. While 83% (net) report recognition of attacks, a slightly greater portion report involvement at the response stage (88% net).

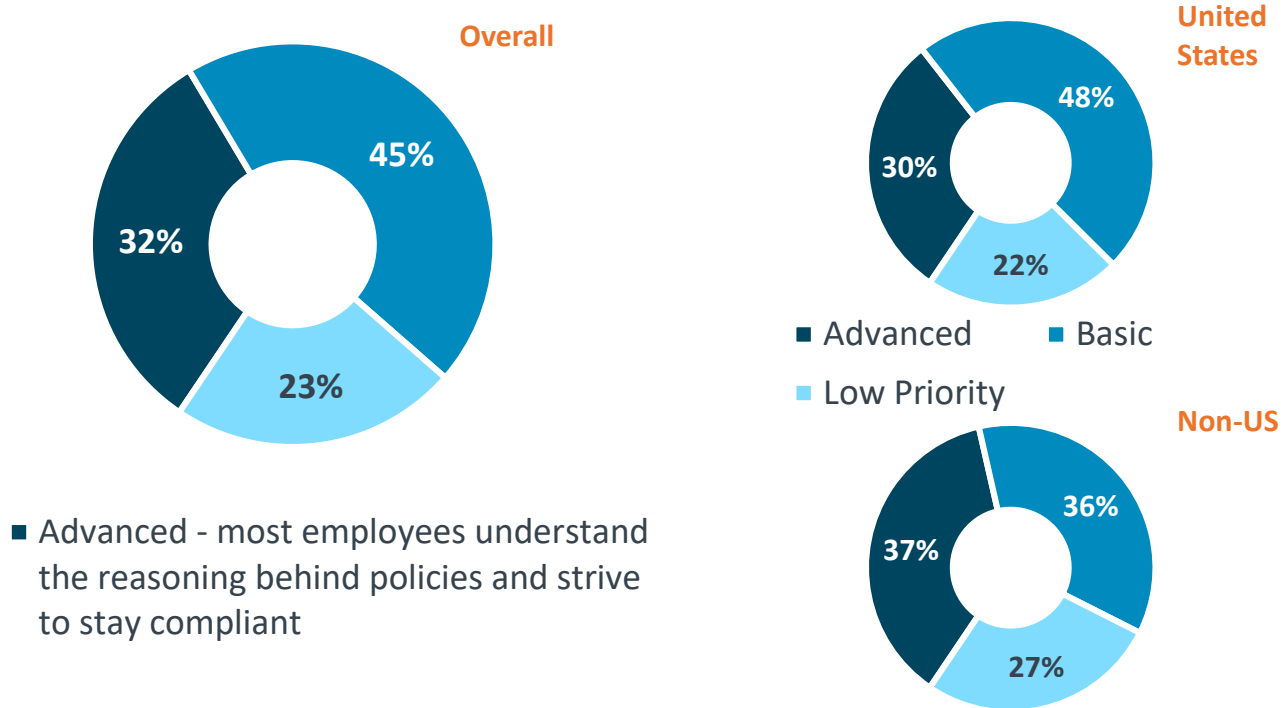
Security training provided for IT support

United States vs. Other Countries (Canada, Ireland, United Kingdom)

Type of Training Provided NET of Some Training + Significant Training	Overall	US	Non-US
General security awareness	79%	81%	73%
Recognize internal threats (e.g. espionage)	68%	71%	63%
Respond to internal threats (e.g. espionage)	68%	70%	62%
Recognize external threats (e.g. phishing, ransomware, DDoS attacks)	75%	76%	73%
Respond to external threats (e.g. phishing, ransomware, DDoS attacks)	72%	74%	67%

Security awareness training provided for employees*

More than three-quarters report their organisation provides its employees with at least basic security awareness training and/or certification to help manage security issues (77% NET). Fewer than a third claim to provide an advanced level of training (32%).

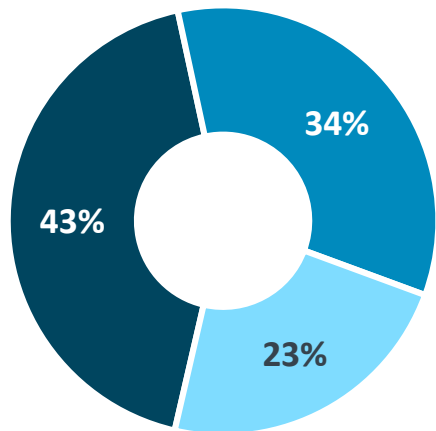


*All employees, including non-IT workers

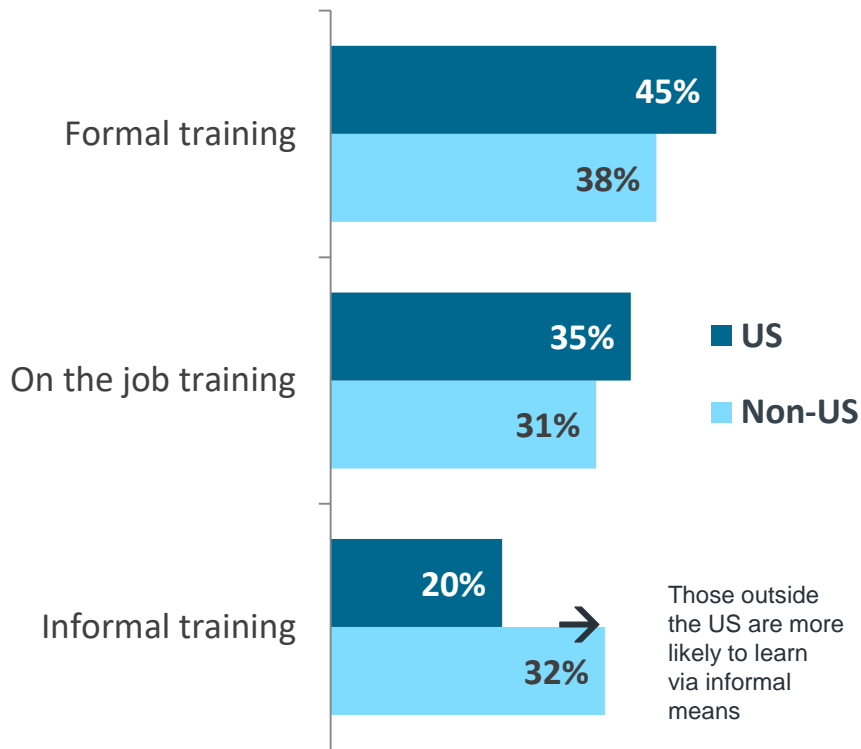
Source: CompTIA IT Security and Support | Overall results, n=439 IT pros

How IT professionals primarily train for IT security

About 4 in 10 primarily learn about IT security best practices / procedures via formal training such as an instructor-led class or online course (43%). Approximately one-third learn it mainly by on the job training (34%).



- Formal training (e.g. instructor-led class, online course)
- On the job training
- Informal training (e.g. word of mouth, assorted experiences)



the practical role of ITSM during a security incident - steps to take

Examples of how support helped in a security incident

Sampling of Comments

- *“A user used their smartphone to connect to the Wi-Fi and it was not protected and support staff spotted an intrusion near the same time as the connection and prevented malware from being installed.”*
- *“Our help desk workers read and recognized unauthorized login attempts in router logs and reported them to the network administrator the network administrator was able to add firewall rules to block the attempts.”*
- *“Callers reporting questionable activity to Service Desk and they recognized the trend in questions from users.”*
- *“Identified a bitcoin mining software running on a server and utilizing resources in task manager.”*
- *“Our organization has been the target of multiple phishing attacks in the past year. We have utilized our helpdesk to communicate with end-users and provide user education regarding how to spot and avoid phishing scams.”*
- *“Phishing attacks were running rampant in our organization due to a bug with our filtering appliance. Our help desk recognized the issue right away and implemented special training for all staff to identify potential attack vectors.”*
- *“We have active monitoring (IPS and IDS) that will send alerts and alarms as needed to the local support helpdesk for that region. The local helpdesk has a very strict SLE and must respond to such items quickly and thoroughly.”*
- *“We have had several instances where CryptoLocker ransomware has been detected on customer machines by the help desk and traced to the infected computer which was taken off the physical network before shared network drives were infected.”*
- *“WannaCry hit this weekend and our entire field services went out to check pc's.”*

Incident response steps

- Identification
- Classification
 - Known threats vs. unknown threats
 - Zero day
 - Advanced persistent threat
- Types of data impacted
 - Personally Identifiable Information (PII) and Personal Health Information (PHI)
 - Credit card information
 - Accounts
- Corrective actions
- Incident summary report

Q: What are the most important security skills required in your organization?

- **59%** Incident response skills
- **41%** Detection of abnormal system behaviors



Incident response steps (cont'd)

- Containment activities
 - Segmentation
 - Isolation
 - Removal
 - Eradication
 - Sanitization
 - Reconstruction/reimage
 - Secure disposal
- Inform the appropriate workers and employees
- Communication

Where does the help desk fit in?



Help desk / service desk input for the security team

- End point security and baselining
 - Provide end point information
 - End point information *state*
- The difference between:
 - Failed applications and an attack
 - Routing loops and an attack
 - “I can’t access that site”
and a DNS-based attack
 - “Why doesn’t the printer work”
and a malware-based attack

Can help avoid “baking in” end point problems to the baseline information

Why aren’t help desk metrics analyzed from a “big data” perspective?

Stories about the “kill chain”

Little to nothing can be done as we support a Government organization. All security matters are handled at levels higher than the help desk / service desk. Group policies, HBSS, OS lock down's, non use of external device storage, non running of any exe's not approved etc..., are so tight that security incidents are rare. If one happens internally, whether accidental, purposeful or other wise, the employee is reprimanded and usually fired or removed from network access (this includes non-IT and IT employees). There is little to nothing that the local IT staff can address as far as security.

Phishing attacks were running rampant in our organization due to a bug with our filtering appliance. Our help desk recognized the issue right away and implemented special training for all staff to identify potential attack vectors.

After the recent Ransomware attack. It was found that many of our servers had not been patched in 3yrs or more !. The Service Desk had to assist in getting over 100 servers fully patched. The issue lay with the Infrastructure team and their poor management of the server estate.

What do we protect?

- **The data?**

- Focus on IP
- Privacy

- **The device?**

- Focus on infrastructure
- What about data?

- **The system?**

- ITIL-oriented
- Compliance

- **The company?**

- Policy-based
- Lose the trees for the forest



USER FRIENDLY by ILLIAD



Different perspectives – who is right?

Top Examples

- Networking / network security
- Passwords
- Education / knowledge, including staying updated on trends and threats
- Training / certification
- Firewalls
- Identity & access management
- Policies
- Awareness / attention to detail
- Anti virus
- Common sense / critical thinking / logic / reasoning
- Encryption
- Customer service / friendliness / patience / professionalism
- Communication
- Troubleshooting
- Patch management
- User education
- Social engineering
- Malware
- Recognition
- Prevention / proactiveness

**the practical role of the ITSM professional –
today and tomorrow**

Handling dreaded customer support comments/questions

Here are some, as found by our respondents

- “I followed the antivirus instructions, but now I get a new login screen. Can you help?”
- “Can you help me download my e-mail to my new phone?”
- “How long will it take before you can replace the broken screen on my tablet/phone?”
- “Could you explain this weird code that I keep seeing when I try to go up to the Intranet?”
- “I think I’ve gotten hacked. My password worked on Friday, but now I can’t get in.”
- “Whenever I launch an application on my computer, the screen shows something completely different.”

Ransomware

Explain policy, then do it?

Fix? *Replace!*

What code? 404?

**Password reset!
Didn’t heed notices**

Switched monitor?

Help desk stories

- “My computer won't let me log in”
- Our printers keep having the same problem, company-wide
- “There’s a new login screen”
- ITSM pros setting up bitcoin operations
 - For payment in bitcoin once an attack happens
 - For illicit reasons
- Additional Stories:

A client was targeted by a social engineering con made through a telephone call. My company had already warned them of similar attacks, and they were able to recognise the danger and hang up on the caller. My company was then called in to perform an audit, as the client had accidentally given up remote control of their computer for a few seconds before they hung up (by being tricked into doing so via command prompts).

“We had callers reporting questionable activity to Service Desk and they recognized the trend in questions from users.”

Consistent scan of the end user laptops to check for malicious software, malware, spyware, and ransom wars. We are always checking to make sure all threats get addressed rapidly. User recently had 300 malicious add-in and malware that required us to take the laptop into quarantine.

More stories

Help desk was able to identify a malicious e-mail that assisted in leaking staff e-mail distros and account info. They quickly responded by provisioning accounts that were affected and reduced any further employees befalling the same mistake.

Limited to identification of issue and following predetermined company policies.

Noticed numerous emails related to the Google Docs spoof attack and notified all employees to be aware of the situation and how to rectify it if they fell victim to it.

Our organization is passive in incident response. Meaning once the Information Assurance (IA) team is notified by the regional command that a computer has been compromised, they contact us. We are tasked to secure the machine, disconnect network communications, ensure the machine stays on but is not logged into. IA arrives on scene a few days later to conduct an investigation on the machine.

Phishing attacks were running rampant in or organization due to a bug with our filtering appliance. Our help desk recognized the issue right away and implemented special training for all staff to identify potential attack vectors.

Previously, phishing (whaling) worm entered the network and network resources took a hit. Our personnel was instrumental in tracking down the infected devices and set a remediation plan in place to further stop the attack. Also instrumental in providing training within the organization.

Where the help desk can – and does – fit in

The biggest problem with security is the policies that were set many years ago and they don't make much sense in this present day. The method that we patched the "WannaCry" Ransomware was very archaic. We couldn't mass deploy the update. We had to manually and personally install the patch with USB Flash drives with over 250 Computers in the office. The IT Support team agree with my sentiments about the way we do things because of the backwards policy. While we were lucky that "WannaCry" didn't hit us, but the fact that it managed to infect and spread on the computers in UK and Australia, it just shows how many companies, or rather the decision makers, don't understand the importance of security.

It's like Gordon Ramsay's Kitchen Nightmare where the Chef is the expert at making an awesome burger but the Owner wants the Chef to make some Crappy burger instead because the Chef is being paid by the Owner.

The help desk often sees phishing attempts and people trying to gain unauthorized access to systems. Usually they often see a flaw in a supported or recently released application because of the number of trouble calls that come in. Tier II and III personnel then get involved with application developers to resolve the issues before they can be exploited. Service technicians doing vulnerability scans can isolate effected systems and take them offline until patching can be done. If an incident occurs, support techs provide investigative assistance with HDD forensic technicians

The company I'm in needs a policy overhaul to improve security. Our CEO even has some distrust with IT because of his lack of understanding in IT security. Our VP of IT seems to be somewhat stuck in the 2000-2010 era. It's hard for us to convince them of change because the rest of the IT team understand the importance of security.

Suggestions for support / help desk to implement

Sampling of Comments

Better / More / Ongoing Training, Including for End Users

- *“Educating everyone in the company about threat awareness and how to avoid it.”*
- *“Greater training and awareness of critical nature of being first contact with security issues.”*
- *Additional continued training and awareness, updated policy and procedures.”*
- *“Encourage stronger passwords, locking computer when away from keyboard, aware of phishing emails, and personal responsibility for PII.”*
- *“By training up all support / help desk and service desk staff to combat all cyber security threats to the company.”*
- *“Better security training as it relates to hardware, software and network for first responders, normally help/service desk staff.”*
- *“Keep up to date with threats and maybe do simulated attacks.”*
- *“More training, continuous learning, continuous updates on latest attacks.”*

More / Better Communication / Collaboration Across Teams

- *“Have better communication with the infrastructure, security, server teams. In our organization it is divided in that way.”*
- *“More communication with employees on procedures and incident response.”*
- *“Formal training on remediation and more open communication between towers.”*

Improved / Quicker Ability to Resolve / Prevent Issues

- *“Provide tools to analyze systems in a fast and effective manner without hindering customer's usage.”*
- *“More reactive to alerts and the ability to act on those independently depending on the severity.”*
- *“Ability to mitigate and contain the issues rather than just to escalate (which gives time for the malware to do more damage/replicate over network/etc.).”*

Questions?



Thank you!

James Stanger

jestanger@comptia.org

+1 (360) 970-5357

Twitter: @jamesstanger

Skype: stangernet

Latest articles and blog entries:

4 reasons Employers Look for Certified Staff
<https://tinyurl.com/y769uq4d>

Don't Hack Me, Bro!
<http://www.admin-magazine.com/Archive/2016/35/Implementing-custom-security-frameworks-with-Bro>

5 reasons your company can't hire a cybersecurity professional, and what you can do to fix it
<http://www.techrepublic.com/article/5-reasons-your-company-cant-hire-a-cybersecurity-professional-and-what-you-can-do-to-fix-it>

The old has become new again
<https://certification.comptia.org/it-career-news/post/view/2017/02/24/rsa-report-the-old-has-become-new-again>