ISACA®

Trust in, and value from, information systems

CYBERSECURITY:
ISSUES AND ISACA'S RESPONSE

June 2014

KEY TRENDS AND DRIVERS OF SECURITY

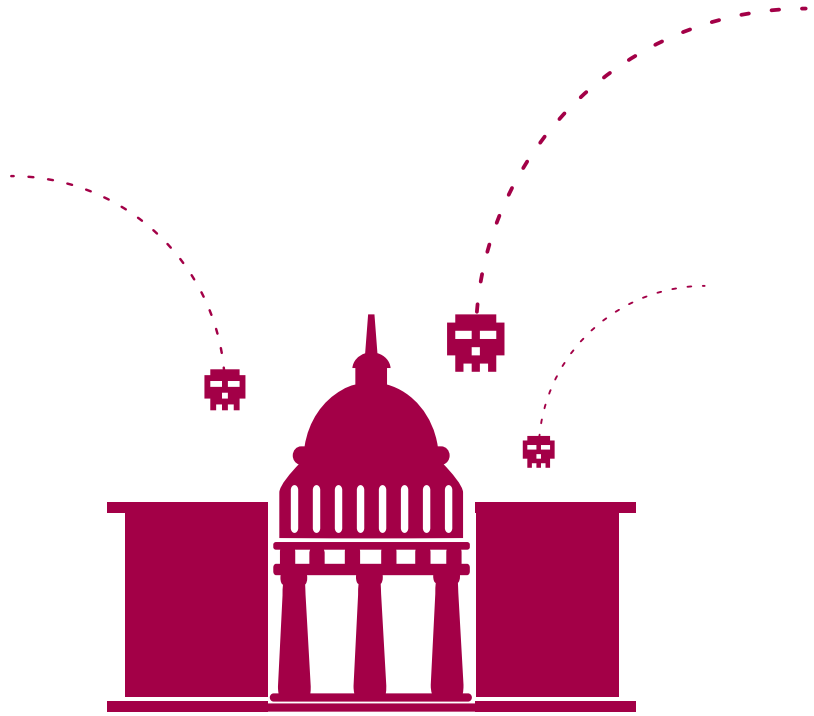
Consumerization	Emerging Trends	Continual Regulatory and Compliance Pressures
• Mobile devices • Social media • Cloud services • Nonstandard • Security as a Service	• Decrease in time to exploit • Targeted attacks • Advanced persistent threats (APTs)	• SOX, PCI, EU Privacy • ISO 27001 • Other regulations

THE WORLD IS CHANGING

The 2010 Google Aurora attack forever changed the way we look at Internet security. This large-scale, sophisticated attack showed us that all sectors, from private to public, are vulnerable to a new class of security breach:

The Advanced Persistent Threat

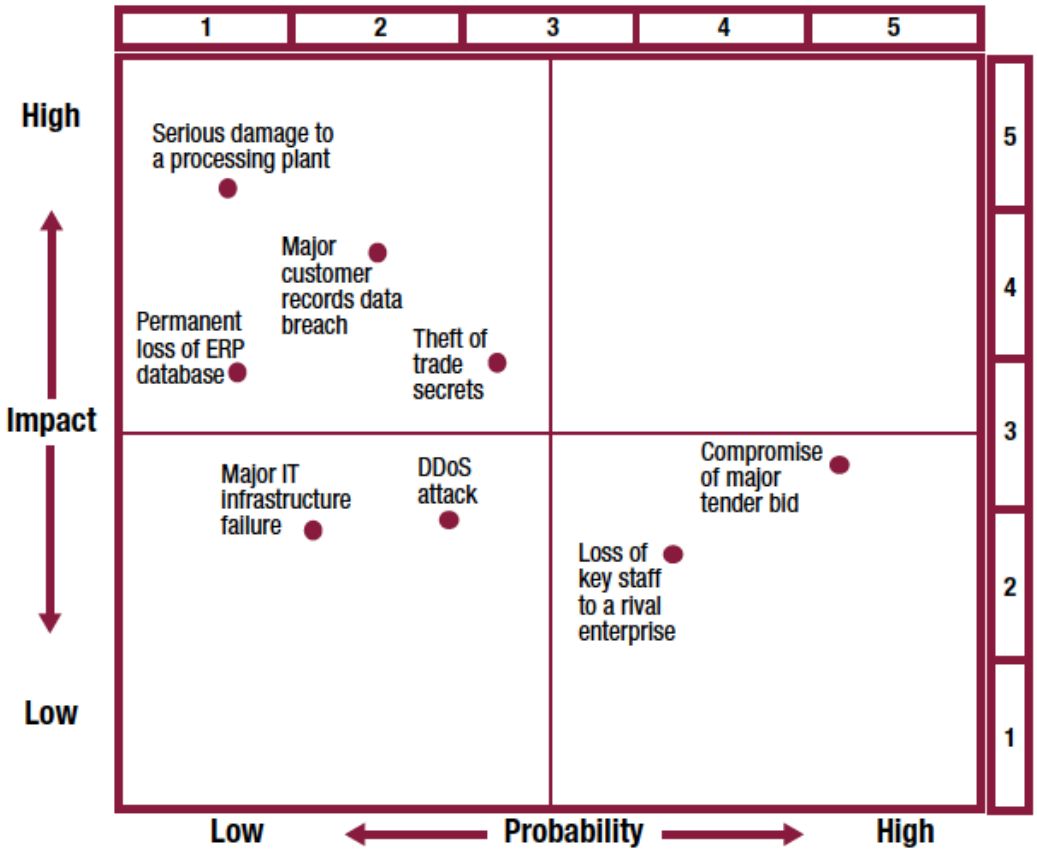
WHAT IS AN ADVANCED PERSISTENT THREAT?



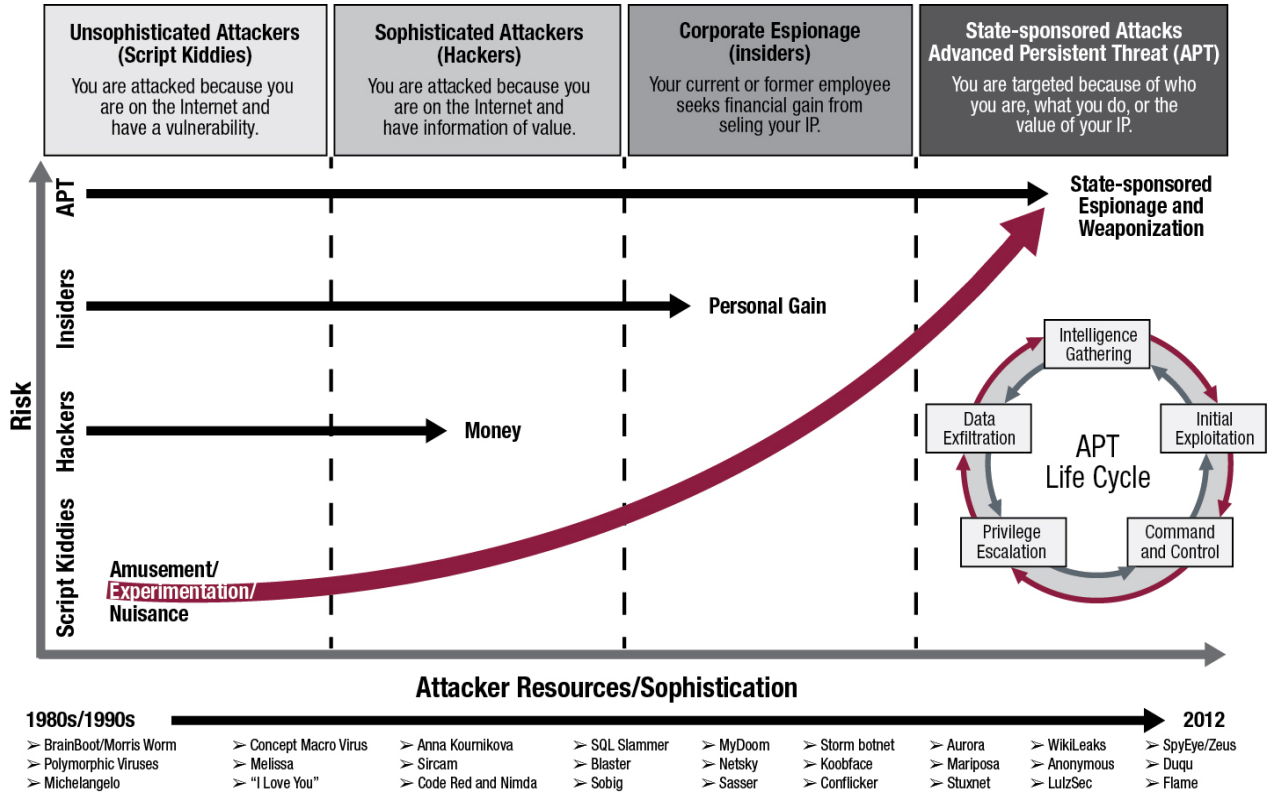
ADVANCED, STEALTHY AND CHAMELEON-LIKE in its adaptability, APTs were once thought to be limited to attacks on government networks.

However, APTs are commonplace and can happen to any enterprise. Repeated pursuit of objectives, adaptation to defenders and persistence differentiate APTs from a typical attack. Primarily, the purpose of the majority of APTs is to extract information from systems—this could be critical research, enterprise intellectual property or government information, among other things.

FIGURE 06 APT Risk Assessment Heat Map Example



THE WORLD IS CHANGING



ISACA
Trust in, and value from, information systems

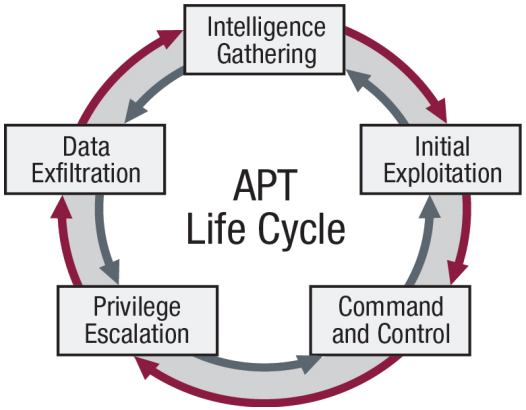
ADAPTIVE ATTACK VECTORS

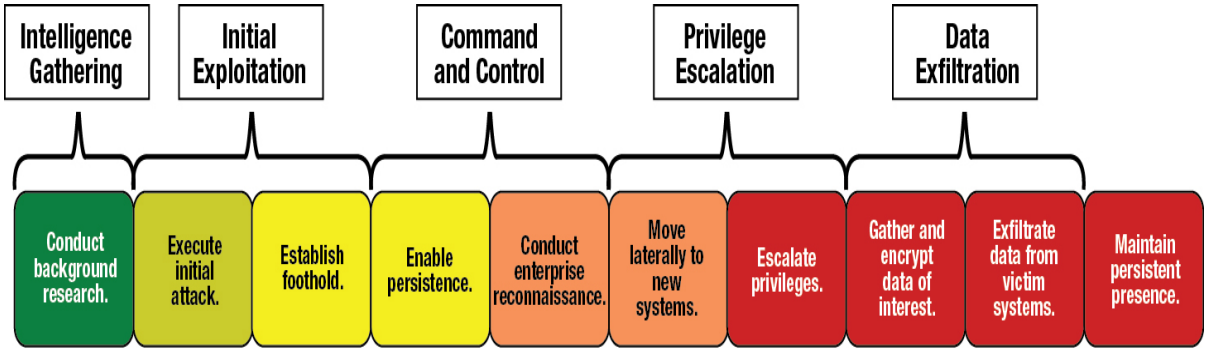
The threat landscape will continue to evolve as attackers adapt new and innovative attack methods to existing or adaptive attack vectors while defenders deploy new defense strategies.

Security Issue	Security Solution	Adaptive Attack Vector
Single-factor authentication (e.g., something you know, such as a user ID and a password) is too weak; passwords are easily compromised or guessed.	Multifactor authentication—something you know (user ID/password) plus something you have (password retrievable from a token that changes at regular intervals based on strong encryption algorithms)	Break into the token vendor (RSA, March 2011) and steal the encryption keys that are used by the real target (Lockheed Martin, May 2011).
There are thousands of malware writers, some of whom masquerade their code as being from a trusted developer.	Digital certificates used to "sign" code from a vendor so that the code can be trusted	Break into a credible vendor whose software is run on almost every computer (Adobe) and use its code-signing infrastructure to sign the malicious code (September 2012).
The antivirus approach (defining what "bad" software is and blacklisting or quarantining it) is not able to keep pace with malware writers. There are more than 200,000 new blacklist signatures each day.	Application whitelisting (defining what is "good" and assuming everything else is "bad")	Break into the application whitelisting vendor (Bit9) and have its code-signing infrastructure sign the malicious code so that it is effectively on the whitelist (February 2013).

THE APT LIFE CYCLE

History shows that most sophisticated attackers, regardless of their motives, funding or control, tend to operate in a certain cycle and are extremely effective at attacking their targets.





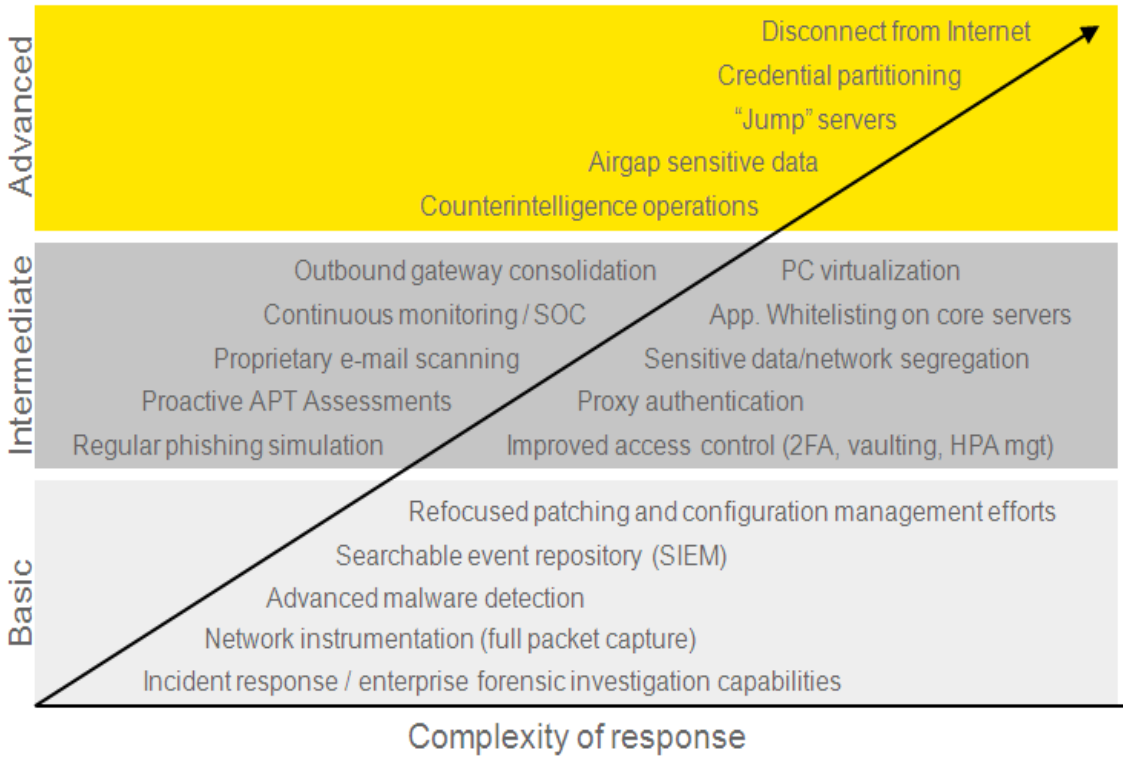
APT MODUS OPERANDI

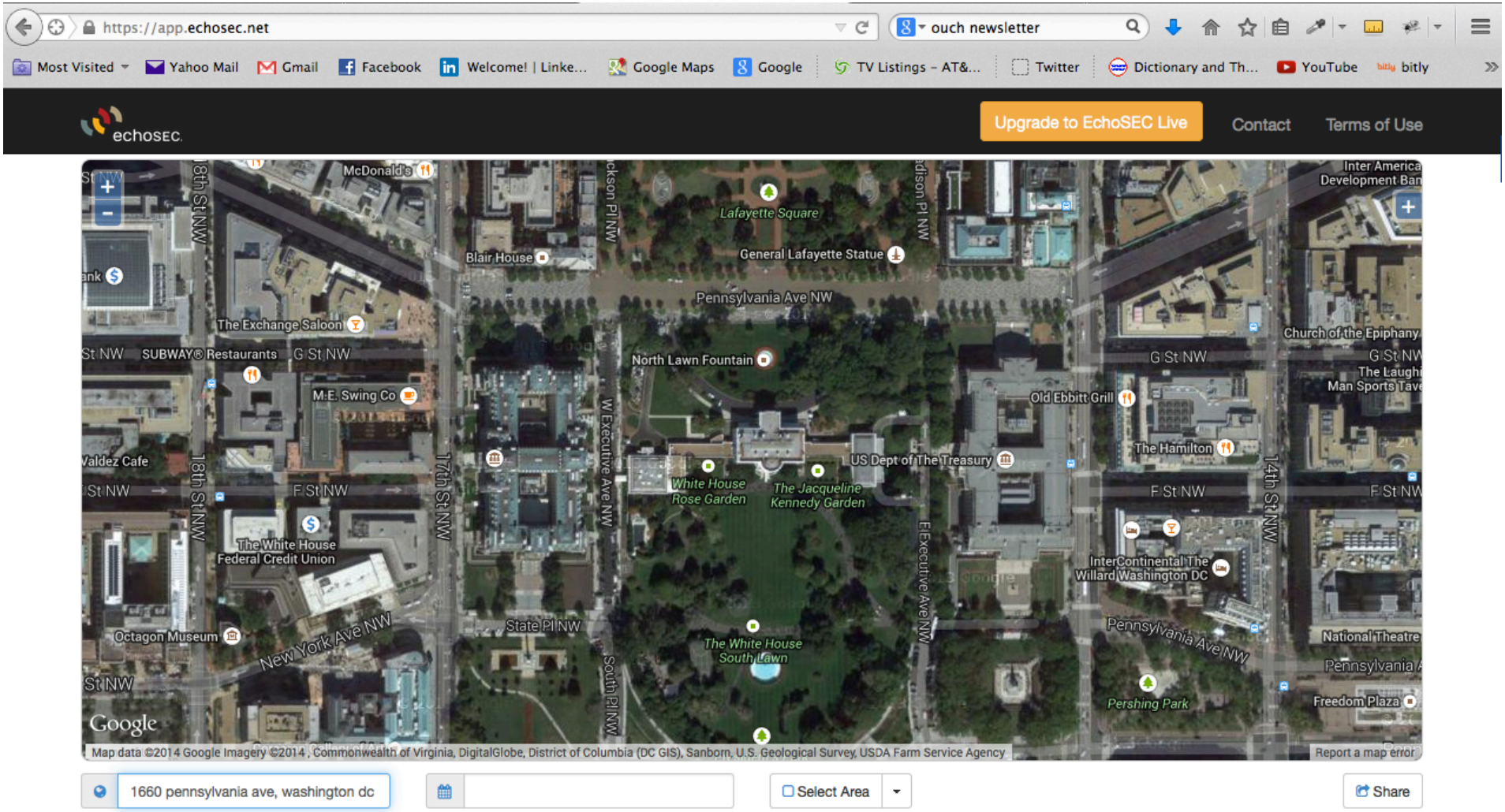
APTs have adapted their tactics, techniques and procedures to the typical information security architecture they find deployed. For example…

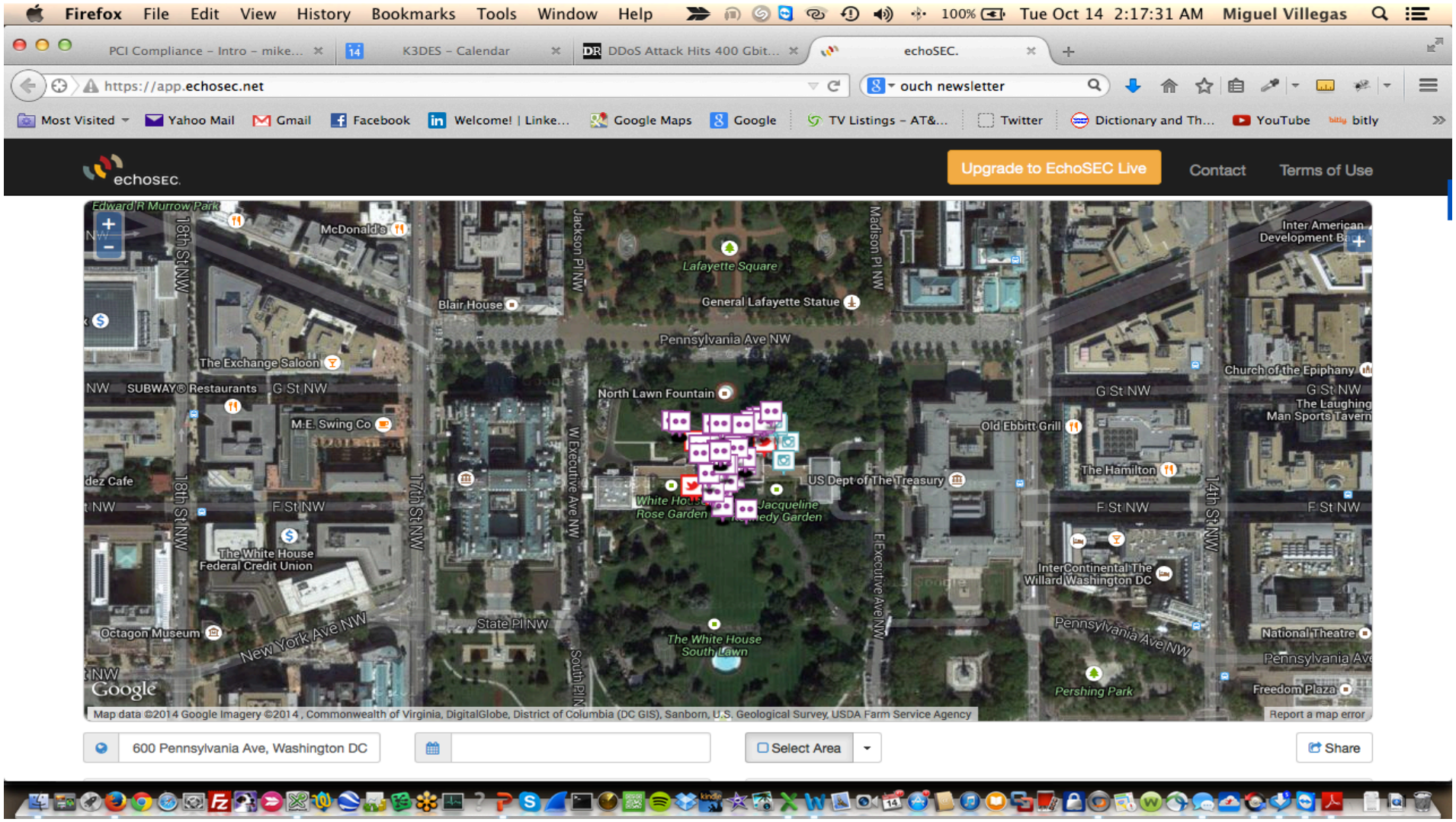
Traditional Security Practice	APT's Modus Operandi
Network boundary/perimeter devices inspect traffic content.	SSL, custom encryption, and password protected/encrypted container files make packet content inspection difficult or impossible.
Network firewalls monitor and assess traffic metadata.	Communication initiated from within the network using standard ports and protocols (HTTP, DNS, SSL, SMTP, etc.).
Host firewalls monitor and assess local traffic metadata.	Initial infection tool adds malware to host firewall white list.
Intrusion detection and prevention systems with real-time assessment and alerting running on servers and workstations.	Communications use common ports and protocols – hide in plain site within obvious/allowed traffic.

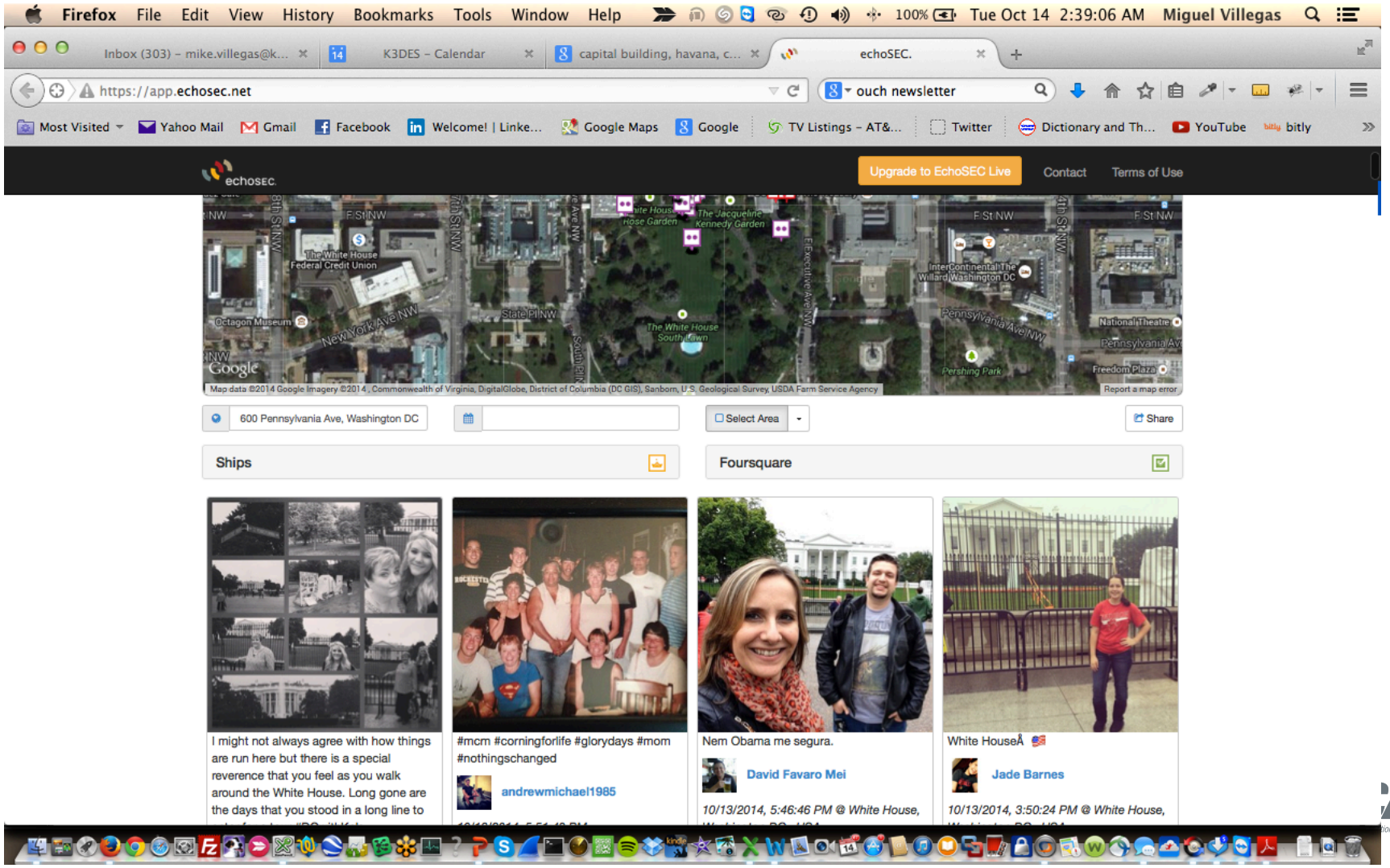
METHODS FOR DEFENDING AGAINST THE APT

Many enterprises implement some of the intermediate-level concepts. Because the APT and other advanced, sophisticated attackers have such a high success rate, it is recommended that every enterprise implement all of the basic concepts.




https://app.echosec.net
ouch newsletter
Most Visited
Yahoo Mail
Gmail
Facebook
Welcome! | Linke...
Google Maps
Google
TV Listings - AT&...
Twitter
Dictionary and Th...
YouTube
bitly
echosec
Upgrade to EchoSEC Live
Contact
Terms of Use
McDonald's
Lafayette Square
Blair House
General Lafayette Statue
Pennsylvania Ave NW
The Exchange Saloon
SUBWAY® Restaurants
G St NW
North Lawn Fountain
M.E. Swing Co
Old Ebbitt Grill
The Hamilton
US Dept of The Treasury
White House Rose Garden
The Jacqueline Kennedy Garden
F St NW
The White House Federal Credit Union
InterContinental The Willard Washington DC
Octagon Museum
New York Ave NW
State Pl NW
The White House South Lawn
Pennsylvania Ave NW
Pershing Park
National Theatre
Freedom Plaza
Church of the Epiphany
Inter America Development Ban
18th St NW
17th St NW
14th St NW
W Executive Ave NW
E Executive Ave NW
Google
Map data ©2014 Google Imagery ©2014 , Commonwealth of Virginia, DigitalGlobe, District of Columbia (DC GIS), Sanborn, U.S. Geological Survey, USDA Farm Service Agency
Report a map error
1660 pennsylvania ave, washington dc
Select Area
Share


Firefox File Edit View History Bookmarks Tools Window Help 100% Tue Oct 14 2:17:31 AM Miguel Villegas
PCI Compliance – Intro – mike...
K3DES – Calendar
DDoS Attack Hits 400 Gbit...
echoSEC.
https://app.echosec.net
ouch newsletter
Most Visited
Yahoo Mail
Gmail
Facebook
Welcome! | Linke...
Google Maps
Google
TV Listings – AT&...
Twitter
Dictionary and Th...
YouTube
bitly
echosec.
Upgrade to EchoSEC Live
Contact
Terms of Use
Edward R Murrow Park
McDonald's
18th St NW
Jackson Pl NW
Lafayette Square
Madison Pl NW
Inter American Development Ba
Blair House
General Lafayette Statue
Pennsylvania Ave NW
The Exchange Saloon
Church of the Epiphany
SUBWAY® Restaurants
G St NW
North Lawn Fountain
The Laughing Man Sports Tavern
M.E. Swing Co
Old Ebbitt Grill
W Executive Ave NW
17th St NW
US Dept of The Treasury
The Hamilton
14th St NW
F St NW
White House Rose Garden
Jacqueline Kennedy Garden
The White House Federal Credit Union
InterContinental The Willard Washington DC
Octagon Museum
New York Ave NW
State Pl NW
The White House South Lawn
South Pl NW
National Theatre
Pershing Park
Freedom Plaza
Google
Map data ©2014 Google Imagery ©2014 , Commonwealth of Virginia, DigitalGlobe, District of Columbia (DC GIS), Sanborn, U.S. Geological Survey, USDA Farm Service Agency
Report a map error
600 Pennsylvania Ave, Washington DC
Select Area
Share


Firefox File Edit View History Bookmarks Tools Window Help 100% Tue Oct 14 2:39:06 AM Miguel Villegas
Inbox (303) - mike.villegas@k...
K3DES - Calendar
capital building, havana, c...
echoSEC.
https://app.echosec.net
ouch newsletter
Most Visited
Yahoo Mail
Gmail
Facebook
Welcome! | Linke...
Google Maps
Google
TV Listings - AT&...
Twitter
Dictionary and Th...
YouTube
bitly
echosec.
Upgrade to EchoSEC Live
Contact
Terms of Use
The White House Federal Credit Union
Octagon Museum
New York Ave NW
State Pl NW
The White House South Lawn
The Jacqueline Kennedy Garden
InterContinental The Willard Washington DC
Pennsylvania Ave NW
National Theatre
Pershing Park
Freedom Plaza
Google
Map data ©2014 Google Imagery ©2014 , Commonwealth of Virginia, DigitalGlobe, District of Columbia (DC GIS), Sanborn, U.S. Geological Survey, USDA Farm Service Agency
Report a map error
600 Pennsylvania Ave, Washington DC
Select Area
Share
Ships
Foursquare
I might not always agree with how things are run here but there is a special reverence that you feel as you walk around the White House. Long gone are the days that you stood in a long line to
#mcm #corningforlife #glorydays #mom #nothingschanged
andrewmichael1985
Nem Obama me segura.
David Favaro Mei
10/13/2014, 5:46:46 PM @ White House,
White HouseÅ
Jade Barnes
10/13/2014, 3:50:24 PM @ White House,

ISACA'S APT SURVEY

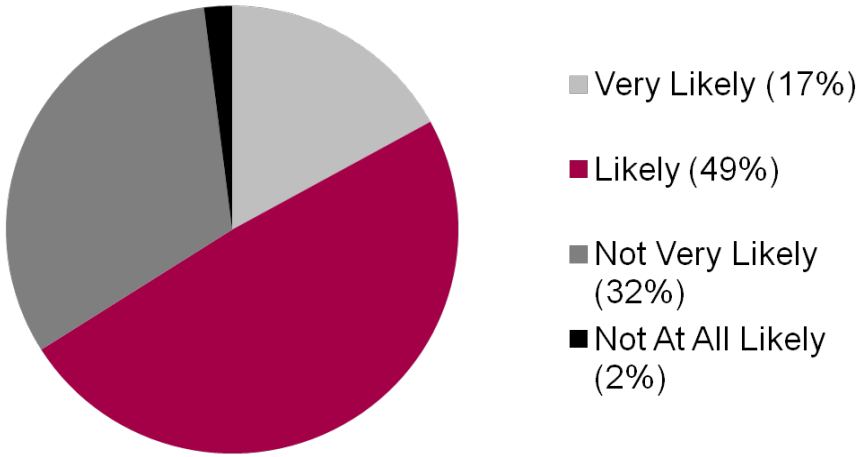
1,220 Individuals Globally; Fielded February 2014

Full Report: 11 June 2014

Because the study's purpose was to measure information security characteristics such as knowledge of advanced persistent threats (APTs), internal controls, internal incidents, policy adherence and management support, the study surveyed those who deal with those issues every day: professionals with information security responsibilities.

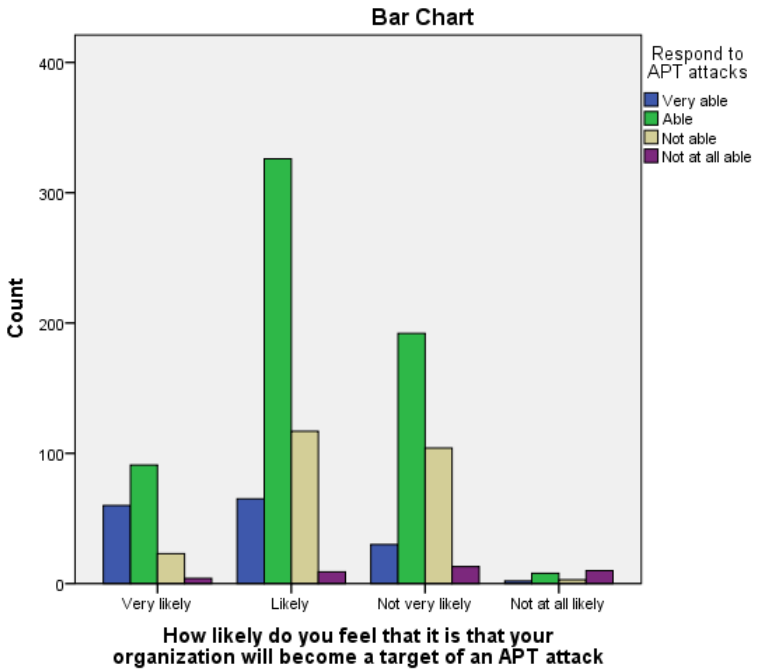
Respondents are still using the wrong controls, such as antimalware, antivirus and firewalls, to defend against APTs. These aren't effective as most of these attacks come from zero-day exploits and the attack vectors are very personalized spear-phishing attacks and now web exploits in the browser. While technology improvements are not clear, behavior is improving, with more organizations making the necessary changes in terms of incident response plans and security awareness training.

- **92% SAY APTS POSE A CREDIBLE THREAT TO NATIONAL SECURITY OR ECONOMIC STABILITY.**
- **1 IN 5 HAVE EXPERIENCED AN APT ATTACK.**
- **66% SAY IT IS LIKELY OR VERY LIKELY THAT THEIR ORGANIZATION WILL EXPERIENCE AN APT ATTACK:**



ISACA
Trust in, and value from, information systems

CROSSTAB OF THOSE WHO FIND AN APT LIKELY AND ABILITY TO RESPOND TO AN APT ATTACK



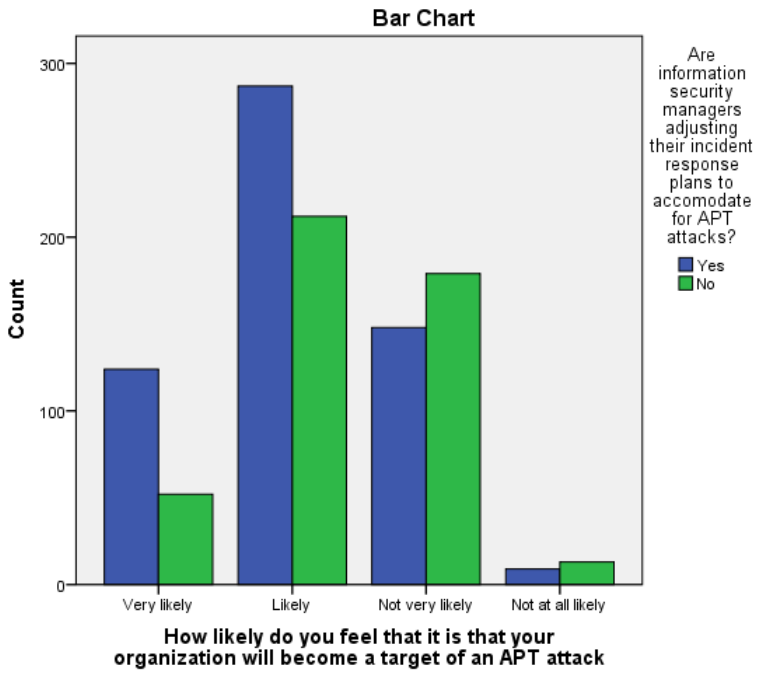
How likely do you feel that it is that your organization will become a target of an APT attack * Respond to APT attacks Crosstabulation

Count

		Respond to APT attacks				Total
		Very able	Able	Not able	Not at all able	
How likely do you feel that it is that your organization will become a target of an APT attack	Very likely	60	91	23	4	178
	Likely	65	326	117	9	517
	Not very likely	30	192	104	13	339
	Not at all likely	2	8	3	10	23
Total		157	617	247	36	1057

ISACA
Trust in, and value from, information systems

CROSSTAB OF BELIEF OF LIKELIHOOD OF BECOMING TARGET AND ADJUSTING INCIDENT RESPONSE PLAN



Crosstab

Count

		Are information security managers adjusting their incident response plans to accomodate for APT attacks?		
		Yes	No	Total
How likely do you feel that it is that your organization will become a target of an APT attack	Very likely	124	52	176
	Likely	287	212	499
	Not very likely	148	179	327
	Not at all likely	9	13	22
Total		568	456	1024

Good news! More than half of organizations who say an APT is likely or very likely to impact them are adjusting their incident response plans to accommodate for APT attacks. In the “very likely to be attacked” category, about 70% are adjusting their plans, and in the “likely” category, 60% have adjusted the plans.

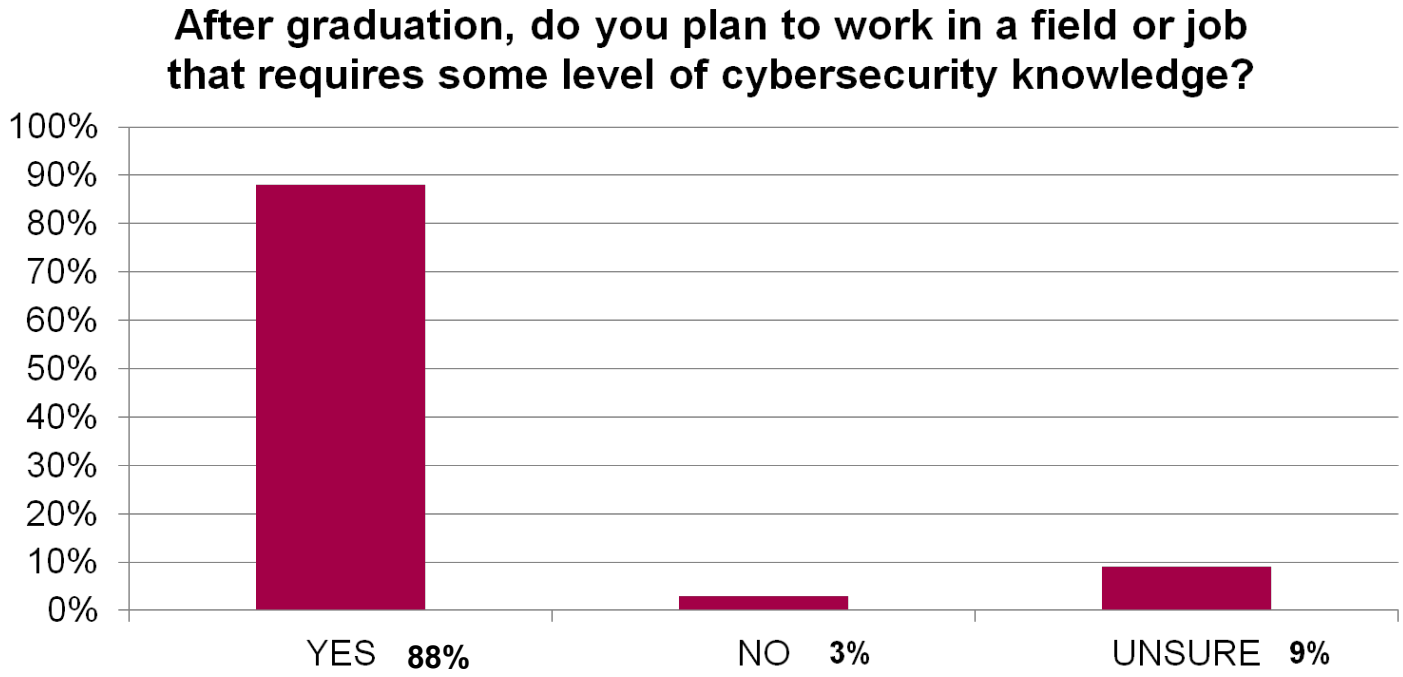
ISACA
Trust in, and value from, information systems

ISACA®
Trust in, and value from, information systems

STUDENT POLL

Security Skills Are Needed, But Most Don’t Feel They Will Have the Skills They Need

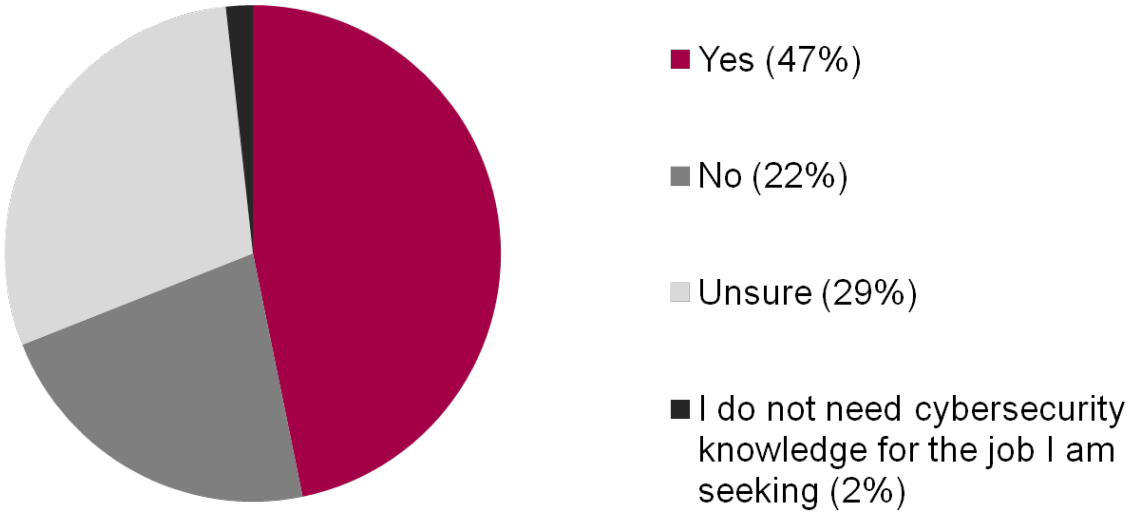
A MAJORITY OF ISACA'S STUDENT MEMBERS (88%) PLAN TO WORK IN A FIELD REQUIRING CYBERSECURITY KNOWLEDGE



ISACA
Trust in, and value from, information systems

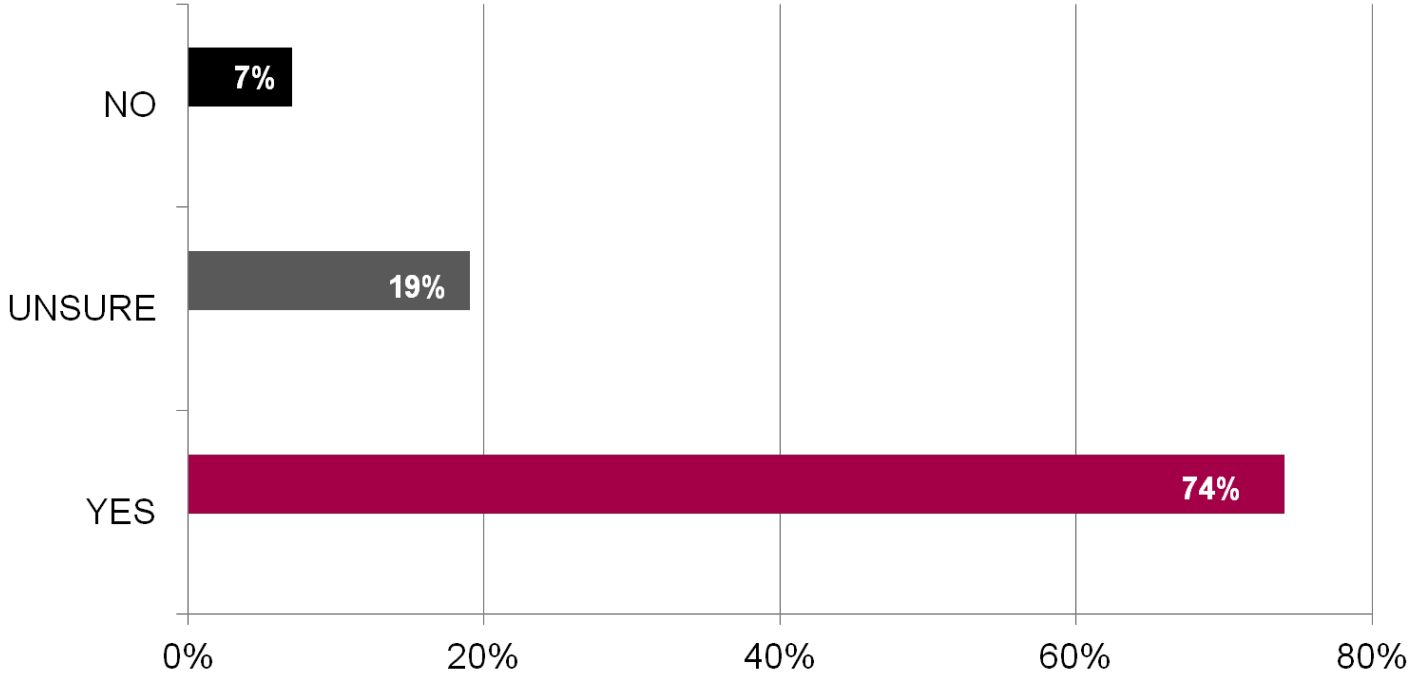
BUT FEWER THAN HALF SAY THEY WILL HAVE ADEQUATE SKILLS FOR THE JOB

Do you feel that you will have adequate cybersecurity knowledge to do the type of job you are seeking when you graduate?

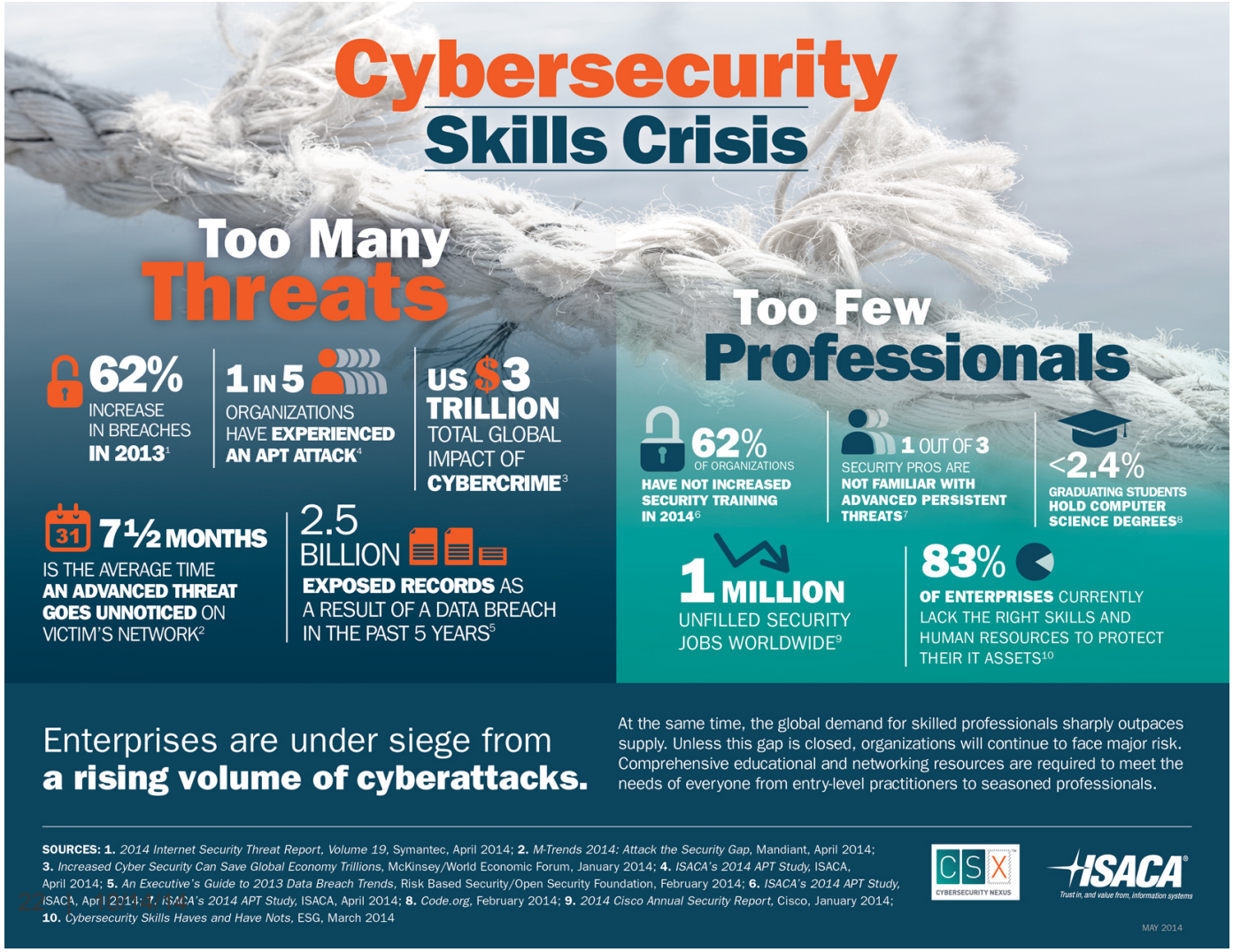


ISACA
Trust in, and value from, information systems

DO YOU PLAN TO PURSUE A CYBERSECURITY RELATED CERTIFICATE OR CERTIFICATION?



ISACA
Trust in, and value from, information systems



ISACA
Trust in, and value from, information systems

CYBERSECURITY NEXUS

www.isaca.org/cyber

…insights and resources for the cybersecurity professional…

…cutting-edge thought leadership, training and certification programs for professionals...

…knowledge, tools, guidance and connections…

ISACA
Trust in, and value from, information systems

CSX ELEMENTS

AVAILABLE NOW

- Cybersecurity Fundamentals Certificate (workshops and exams taking place in Q3; first workshop sold out)
- *Transforming Cybersecurity Using COBIT 5*
- *Responding to Targeted Cyberattacks*
- *Advanced Persistent Threats: Managing the Risks to Your Business*
- APT data
- Cybersecurity webinars and conference tracks (six-part webinar series begins in June)
- Cybersecurity Knowledge Center community

COMING SOON

- Mentoring Program
- Implementation guidance for NIST's US Cybersecurity Framework (which incorporates COBIT 5) and the EU Cybersecurity Strategy
- Cybersecurity practitioner-level certification (first exam: 2015)
- Cybersecurity training courses
- SCADA guidance
- Digital forensics guidance

CYBERSECURITY FUNDAMENTALS KNOWLEDGE CERTIFICATE

Knowledge-based exam for those with 0 to 3 years experience

Foundational level covers four domains:

1) Cybersecurity architecture principles
2) Security of networks, systems, applications and data
3) Incident response
4) Security implications related to adoption of emerging technologies

The exam will be offered online and at select ISACA conferences and training events. The first is in September.

There are no set/regular exam dates throughout the year—the **Cybersecurity Fundamentals Certificate exam is available online**, at your convenience. Simply schedule the date and time that works best for you and your exam will be remotely proctored. Take the exam from the privacy of your own home or office.

The content aligns with the US NICE framework and was developed by a team of about 20 cybersecurity professionals from around the world. The team is involved in all areas of development through content contribution and subject matter expert reviews.

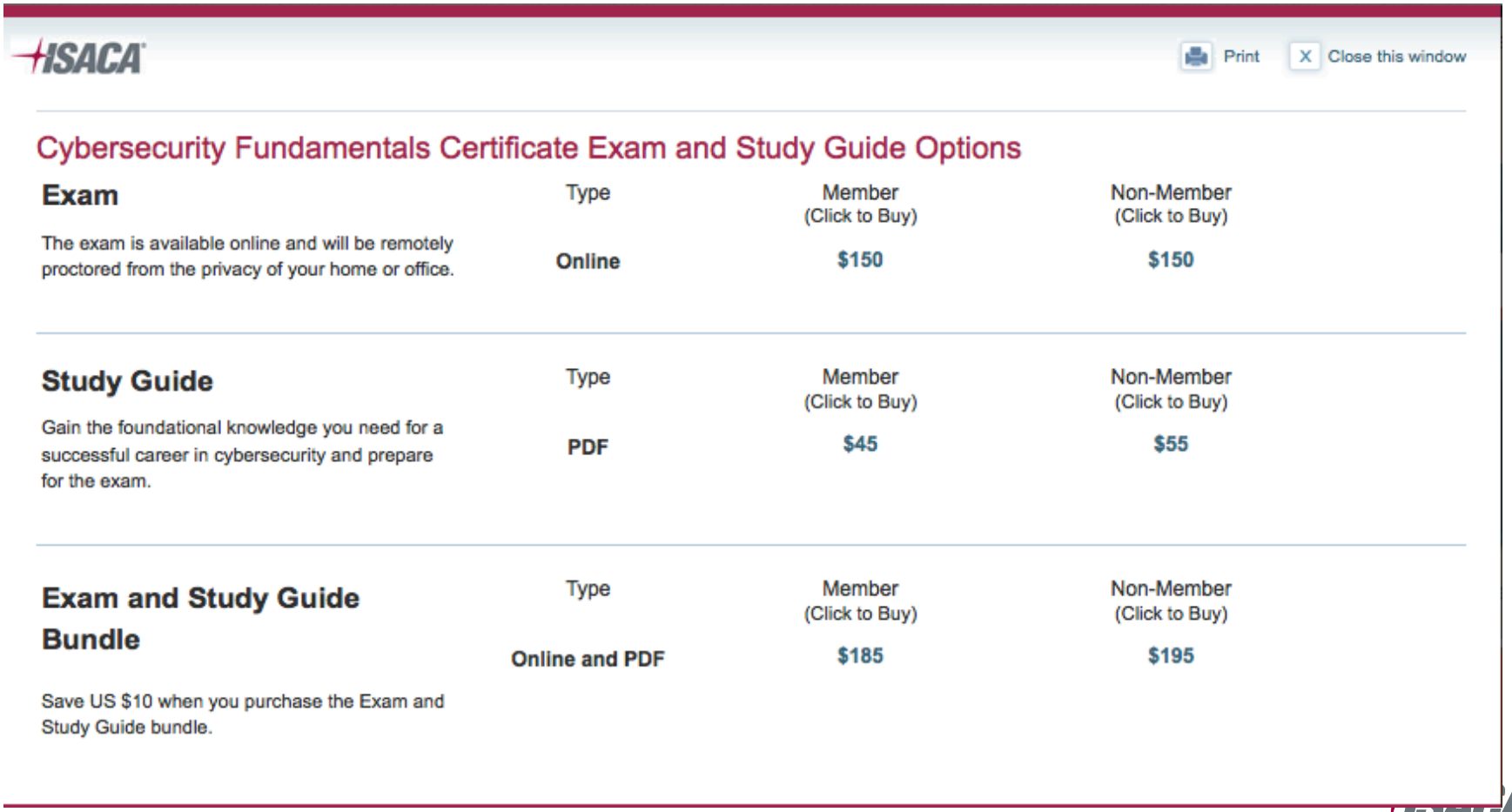
ISACA
Trust in, and value from, information systems

BENEFITS OF EARNING THIS CERTIFICATE

The Cybersecurity Fundamentals Certificate exam tests for foundational knowledge in cybersecurity across five key areas:

- **Cybersecurity concepts**
- **Cybersecurity architecture principles**
- **Cybersecurity of networks, systems, applications and data**
- **The security implications of the adoption of the emerging technologies**
- **Incident responses**

The certificate is particularly relevant for recent college/university graduates, entry level professionals and those looking for a career change to cybersecurity.



ISACA

Print | Close this window

Cybersecurity Fundamentals Certificate Exam and Study Guide Options

Exam

The exam is available online and will be remotely proctored from the privacy of your home or office.

Type	Member (Click to Buy)	Non-Member (Click to Buy)
Online	**$150**	**$150**

Study Guide

Gain the foundational knowledge you need for a successful career in cybersecurity and prepare for the exam.

Type	Member (Click to Buy)	Non-Member (Click to Buy)
PDF	**$45**	**$55**

Exam and Study Guide Bundle

Save US $10 when you purchase the Exam and Study Guide bundle.

Type	Member (Click to Buy)	Non-Member (Click to Buy)
Online and PDF	**$185**	**$195**

CAREER PATH

0-3 years: Cybersecurity Fundamentals Certificate (no experience required; must pass knowledge-based exam)

3-5 years: Cybersecurity practitioner-level certification (coming in mid-2015)

5+ years: Certified Information Security Manager certification (25,000+ professionals certified since inception)

ISACA
Trust in, and value from, information systems

CONTENTS

CYBERSECURITY TRIAD

ISACA
Trust in, and value from, information systems

Information Security vs Cybersecurity

Information security deals with information, regardless of its format—it encompasses paper documents, digital and intellectual property in people's minds, and verbal or visual communications.

Cybersecurity, on the other hand, is concerned with protecting digital assets—everything from networks to hardware and information that is processed, stored or transported by internetworked information systems. Additionally, concepts such as nation-state-sponsored attacks and advanced persistent threats (APTs) belong almost exclusively to cybersecurity. It is helpful to think of cybersecurity as a component of information security.

Therefore, to eliminate confusion, the term cybersecurity will be defined in this guide as protecting information assets by addressing threats to information processed, stored and transported by internetworked information systems.

TRANSFORMING CYBERSECURITY USING COBIT 5

Eight Key Principles:

1. Understand the potential impact of cybercrime and warfare on your enterprise.
2. Understand end users, their cultural values and their behavior patterns.
3. Clearly state the business case for cybersecurity and the risk appetite of the enterprise.
4. Establish cybersecurity governance.
5. Manage cybersecurity using principles and enablers. (The principles and enablers found in COBIT 5 will help your organization ensure end-to-end governance that meets stakeholder needs, covers the enterprise to end and provides a holistic approach, among other benefits. The processes, controls, activities and key performance indicators associated with each enabler will provide the enterprise with a comprehensive picture of cybersecurity.)
6. Know the cybersecurity assurance universe and objectives.
7. Provide reasonable assurance over cybersecurity. (This includes monitoring, internal reviews, audits and, as needed, investigative and forensic analysis.)
8. Establish and evolve systemic cybersecurity.

ISACA®
Trust in, and value from, information systems

COBIT 5 Information Security Policy Set

Section 2—Knowledge Check

Directions: Select the correct answer to complete each statement below. Use each word only once.

Word Bank

Standards	Vulnerability	Guidelines
Attack Vector	Policies	Risk
Threat	Asset	Patches
Identity Management	Malware	Rootkit
Payload	Procedure	

1. The core duty of cybersecurity is to identify, respond to and manage _____ to an organization's digital assets.
2. A(n) _____ is anything capable of acting against an asset in a manner that can cause harm.
3. A(n) _____ is something of value worth protecting.
4. A(n) _____ is a weakness in the design, implementation, operation or internal controls in a process that could be exploited to violate the system security.
5. The path or route used to gain access to the target asset is known as a(n) _____.
6. In an attack, the container that delivers the exploit to the target is called a(n) _____.
7. _____ communicate required and prohibited activities and behaviors.
8. _____ is a class of malware that hides the existence of other malware by modifying the underlying operating system.
9. _____ provide details on how to comply with policies and standards.
10. _____ provide general guidance and recommendations on what to do in particular circumstances.
11. _____, also called malicious code, is software designed to gain access to targeted computer systems, steal information or disrupt computer operations.
12. _____ are used to interpret policies in specific situations.
13. _____ are solutions to software programming and coding errors.
14. _____includes many components such as directory services, authentication and authorization services, and user management capabilities such as provisioning and deprovisioning.

Section 2—Knowledge Check

1. The core duty of cybersecurity is to identify, respond and manage risk to an organization's digital assets.
2. A(n) threat is anything capable of acting against an asset in a manner that can cause harm.
3. A(n) asset is something of value worth protecting.
4. A(n) vulnerability is a weakness in the design, implementation, operation or internal controls in a process that could be exploited to violate the system security.
5. The path or route used to gain access to the target asset is known as a(n) attack vector.
6. In an attack, the container that delivers the exploit to the target is called a(n) payload.
7. Policies communicate required and prohibited activities and behaviors.
8. Rootkit is a class of malware that hides the existence of other malware by modifying the underlying operating system.
9. Procedures provide details on how to comply with policies and standards.
10. Guidelines contain step-by-step instructions to carry out procedures.
11. Malware, also called malicious code, is software designed to gain access to targeted computer systems, steal information or disrupt computer operations.
12. Standards are used to interpret policies in specific situations.
13. Patches are solutions to software programming and coding errors.
14. Identity management includes many components such as directory services, authentication and authorization services, and user management capabilities such as provisioning and deprovisioning.

Section 4—Knowledge Check

1. Put the steps of the penetration testing phase into the correct order.
   a. Attack
   b. Discovery
   c. Reporting
   d. Planning

2. System hardening should implement the principle of _____ or _____.
   a. Governance, compliance
   b. Least privilege, access control
   c. Stateful inspection, remote access
   d. Vulnerability assessment, risk mitigation

3. Select all that apply. Which of the following are considered functional areas of network management as defined by ISO?
   a. Accounting management
   b. Fault management
   c. Firewall management
   d. Performance management
   e. Security management

4. Virtualization involves:
   a. The creation of a layer between physical and logical access controls.
   b. Multiple guests coexisting on the same server in isolation of one another.
   c. Simultaneous use of kernel mode and user mode.
   d. DNS interrogation, WHOIS queries and network sniffing.

5. Vulnerability management begins with an understanding of cybersecurity assets and their locations, which can be accomplished by:
   a. Vulnerability scanning.
   b. Penetration testing.
   c. Maintaining an asset inventory.
   d. Using command line tools.

Network Management

Network management is the process of assessing, monitoring, and maintaining network devices and connections. The International Organization for Standardization (ISO) network management model defines five functional areas of network management (FCAPS):

- **Fault Management**—Detect, isolate, notify and correct faults encountered in the network. This category analyzes traffic, trends, SMMP polls and alarms for automatic fault detection.
- **Configuration Management**—Configuration aspects of network devices include configuration file management, inventory management and software management.
- **Accounting Management**—Usage information of network resources.
- **Performance Management**—Monitor and measure various aspects of performance metrics so that acceptable performance can be maintained. This includes response time, link utilization and error rates. Administrators can monitor trends and set threshold alarms.
- **Security Management**—Provide access to network devices and corporate resources to authorized individuals. This category focuses on authentication, authorization, firewalls, network segmentation, IDS and notifications of attempted breaches.

“Becoming a successful security practitioner is hard. Ideal candidates are well-rounded and have a solid foundation in networking, operating systems, web technologies and incident response, and an understanding of the threat landscape and risk management.”

Darren Van Booven, CISA, CISM, CISSP, CPA
Chief Information Security Officer, U.S. House of Representatives, and ISACA Member

QUESTIONS?