RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

A CISO's Perspective: Protecting with Enhanced Visibility and Response

SESSION ID: STR-F02

Jay Leek
CISO
Blackstone

Today's World:
It's not a matter of if, but when

Why: Six irrefutable laws of information security

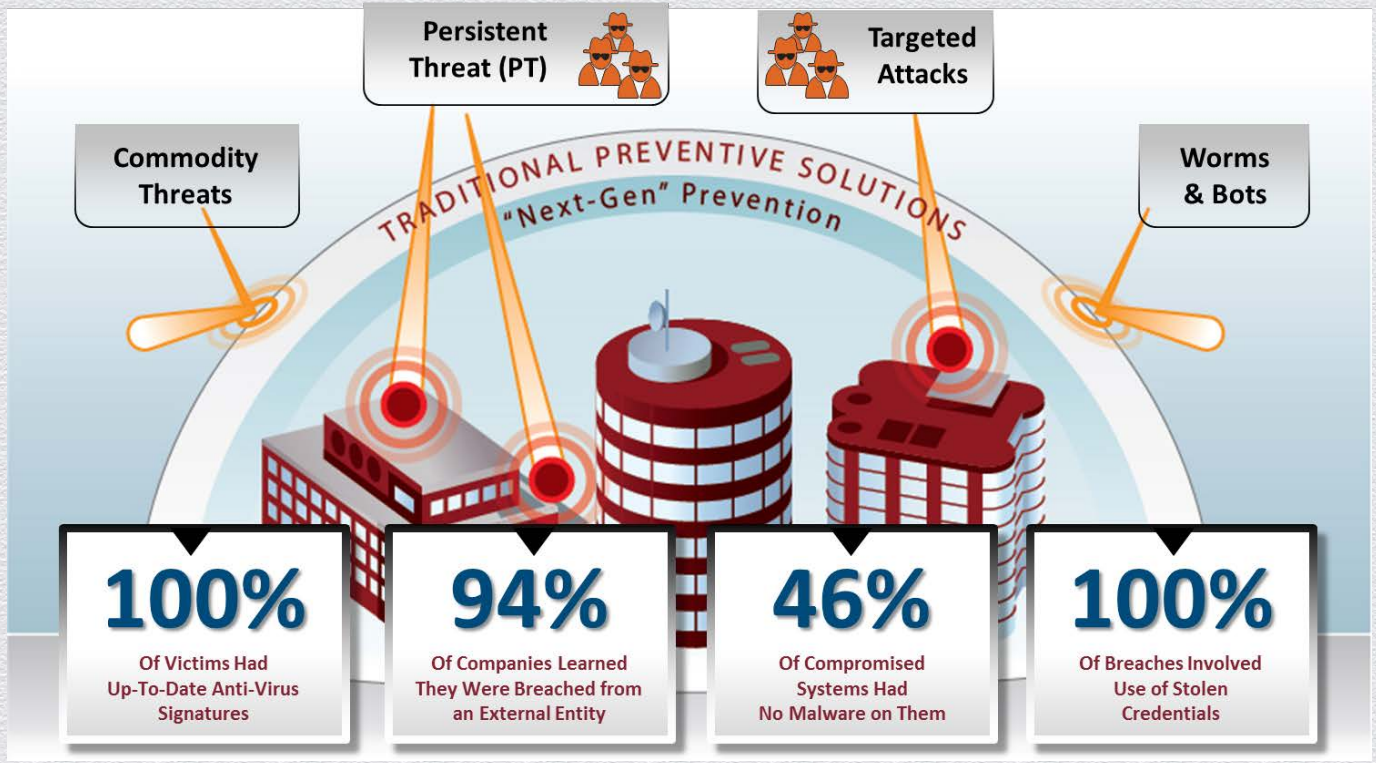
1. Information wants to be free
2. Code wants to be wrong
3. Services want to be on
4. Users want to click
5. Even a security features can be used for harm (e.g. fake AV)
6. The efficiency of a control deteriorates with time

Our environment is naturally working against us

Blackstone

Protect to Enable by Malcolm Harkins, 2012

What: Attacks will eventually bypass defenses given time and persistence



Mandiant M-Trends, 2012

And to further complicated things…

Information security analysts unemployment rate: zero

July 11th, 2011

U.S. information security analysts and computer network architects have enviable job security in an economy marked by nearly 10 percent unemployment.

Of the 12 computer related job classifications the Department of Labor's Bureau of Labor Statistics tracks, Infosec workers reported no unemployment in the second quarter 2011. Computer netwrok architects had a minute 0.5 percent jobless rate in the 2nd quarter and none in the first.

In fact, employment for infosec specialists rose 16 percent from 37,000 to 43,000 in the second quarter.

Infosec analysts plan, implement, upgrade or monitor security measures for the protection of computer networks and information.

Considering the record number of massive government and corporate cyber security breaches in the last quarter, we could use more than a few more infosec specialists.

Why are you telling me what I already know?

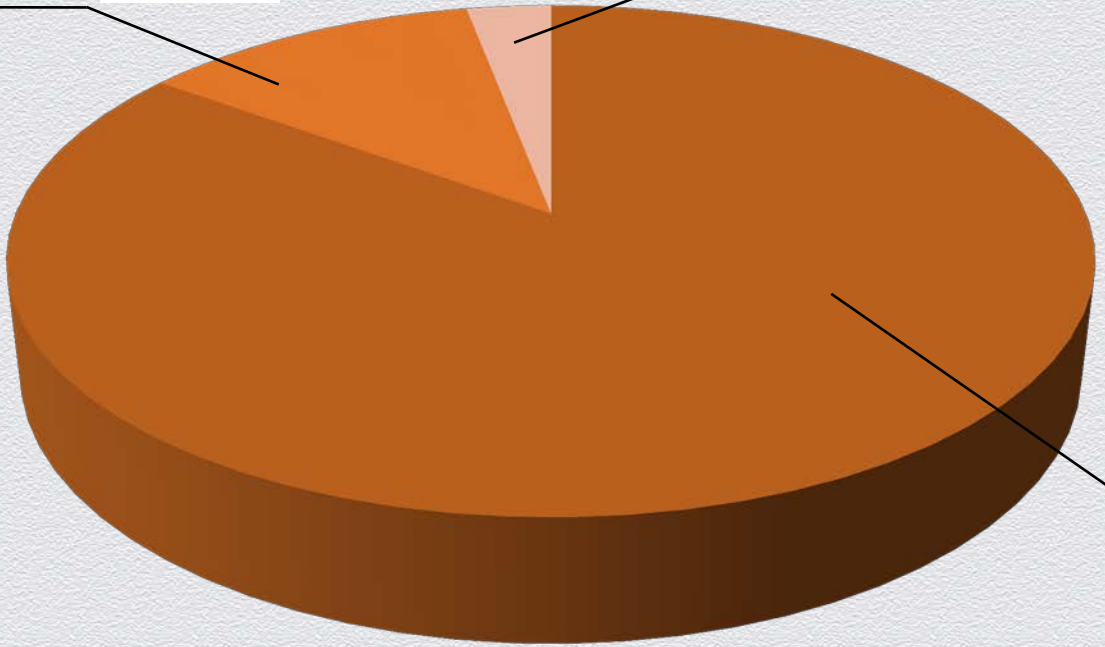
Because something has to change

Blackstone

Information security solutions market today

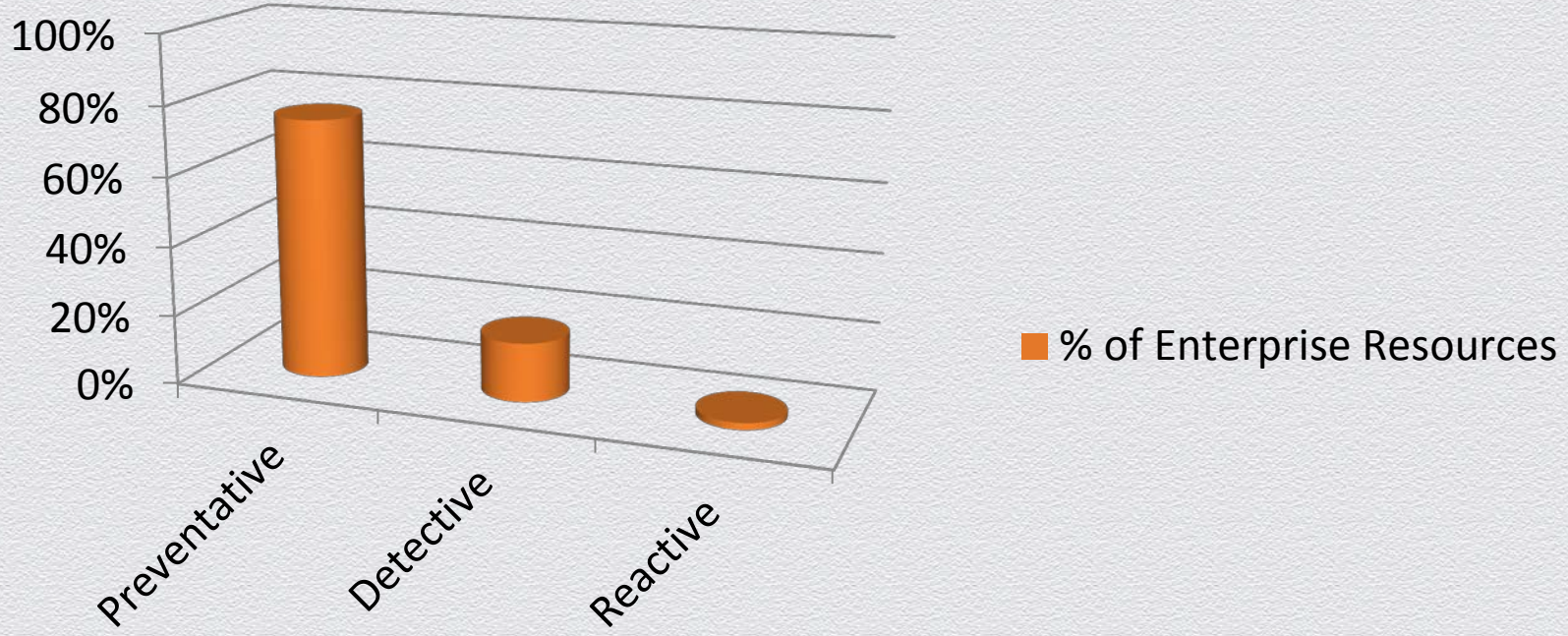
Detective
Mostly Fragmented

Reactive
Largely untapped



Preventative
Saturated by hundreds of products

Typical enterprise resource allocations follow the market



What's wrong this with picture?

Blackstone

#RSAC

RSACONFERENCE2014

The results can be messy

How do you respond when you cannot see?

Guess what is on that plane too?

Blackstone

#RSAC

RSACONFERENCE2014

So what is the answer?

Change #1

Must Improve Our Visibility

Blackstone

#RSAC

RSACONFERENCE2014

Learning from the physical world

Learning from the physical world

Blackstone

#RSAC

RSACONFERENCE2014

Learning from the physical world

Blackstone

#RSAC

RSACONFERENCE2014

Learning from the physical world

Blackstone

#RSAC

RSACONFERENCE2014

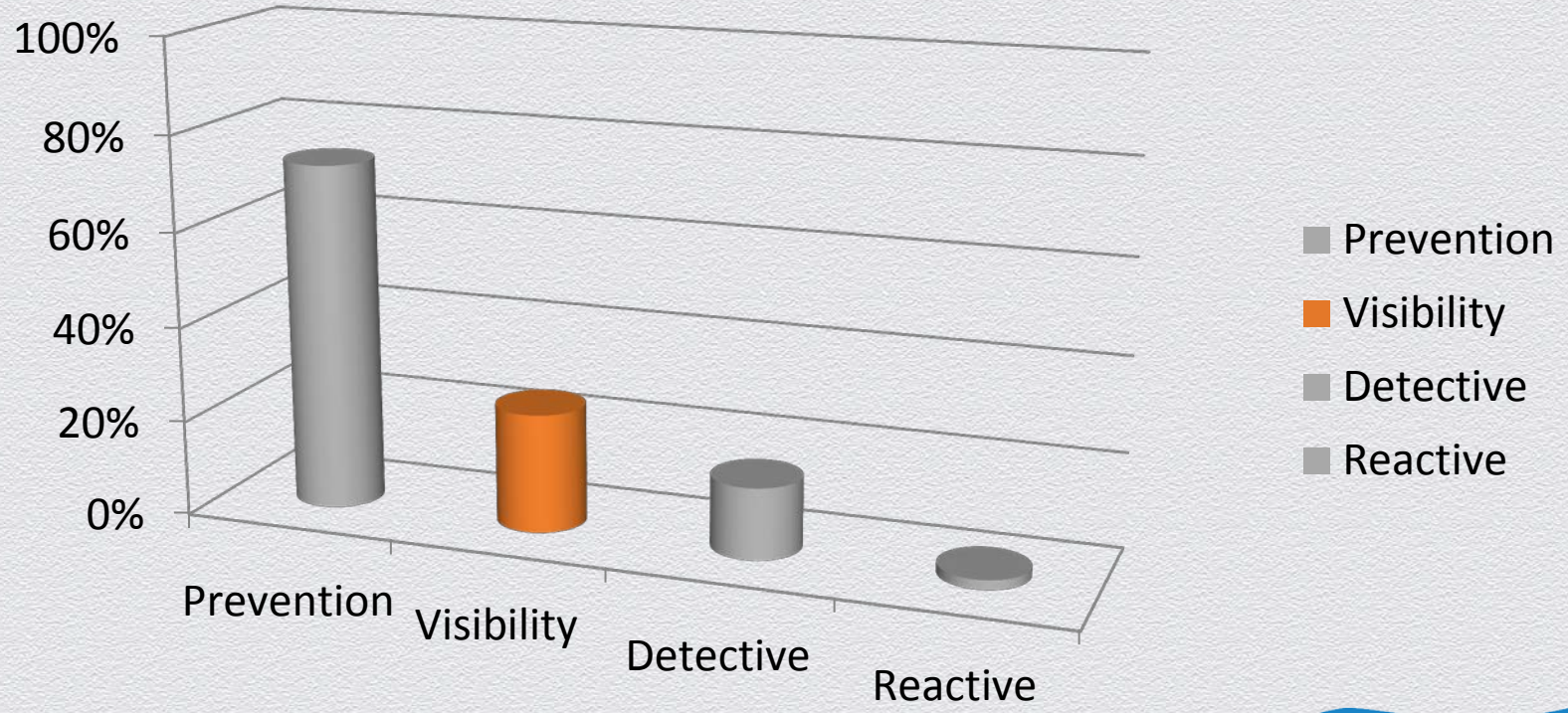
Learning from the physical world

Blackstone

#RSAC

RSACONFERENCE2014

Change #1: Adjusted enterprise resource allocation



Blackstone

Change #2

Need More Intelligence:

Understand what is happening in the world around you, and how it applies to your environment

Must also understand your adversary

Blackstone

What is Intelligence?

- Tracking, analyzing and countering of digital security threats to determine:
  - **Indicators of compromise**
  - **Techniques, tactics and procedures**
    - Are we being targeted?
  - **Threat actors**
    - Who would target us and why?
  - **Vulnerability intelligence**
    - What is being exploited on the wild?
  - **Attack attribution**
    - Is this commodity or targeted?

Example: Cyber Espionage & Cyber Crime Vulnerabilities Exploited

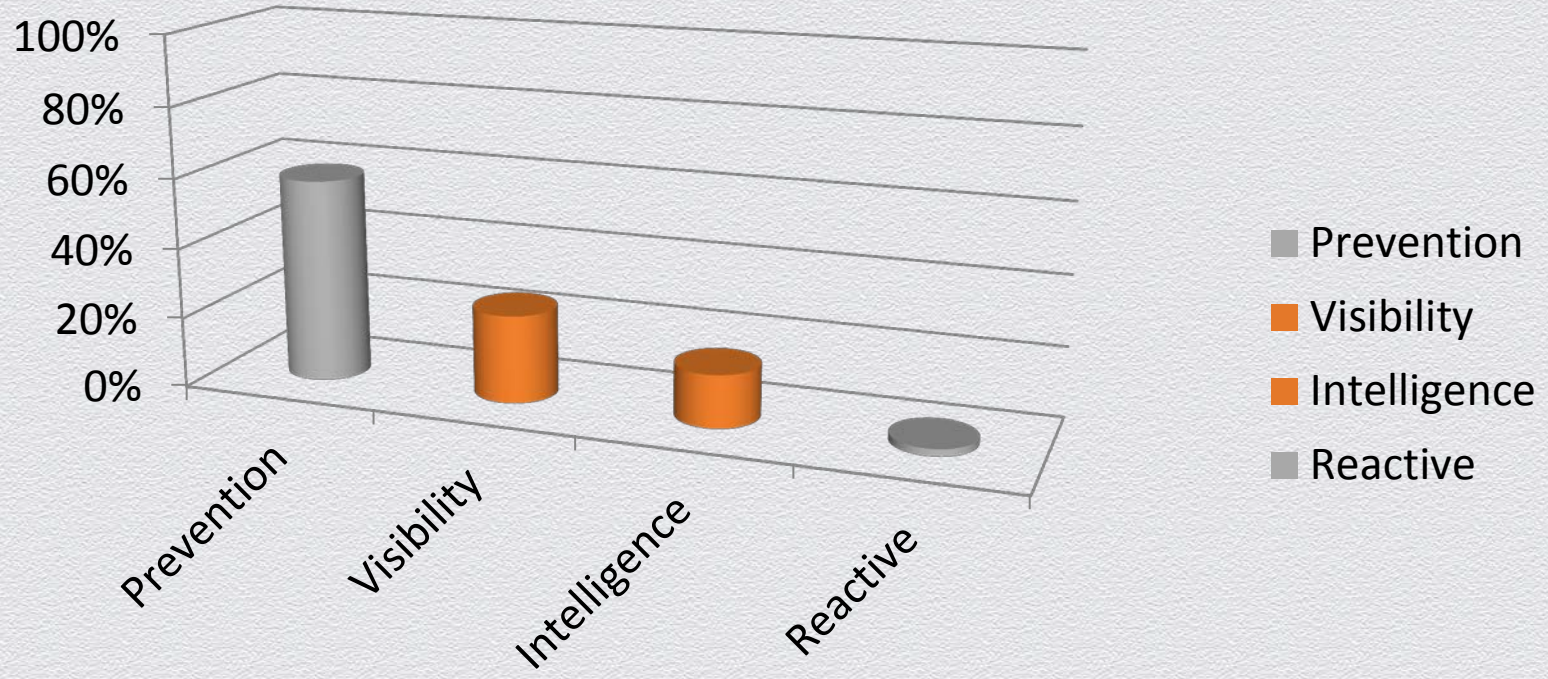
~5000 per year

Blackstone

Mauricio Velazco - Blackstone, 2013
iSight Partners, 2013

Provide actionable recommendations

Change #2: Adjusted enterprise resource allocation



Blackstone

Change #3

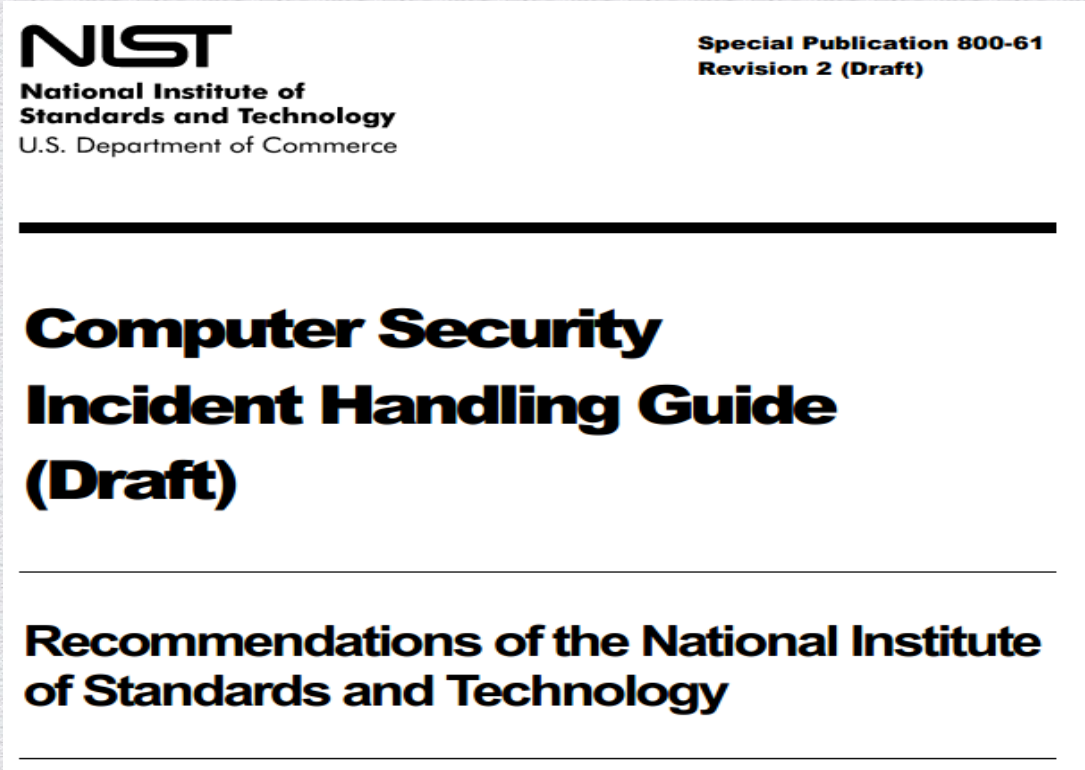
Shift From Reactive To Response:

Now that you are more aware, you need capabilities, process and tools to respond

Planned

Blackstone

This is nothing new, but…



NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Special Publication 800-61
Revision 2 (Draft)

Computer Security Incident Handling Guide (Draft)

Recommendations of the National Institute of Standards and Technology

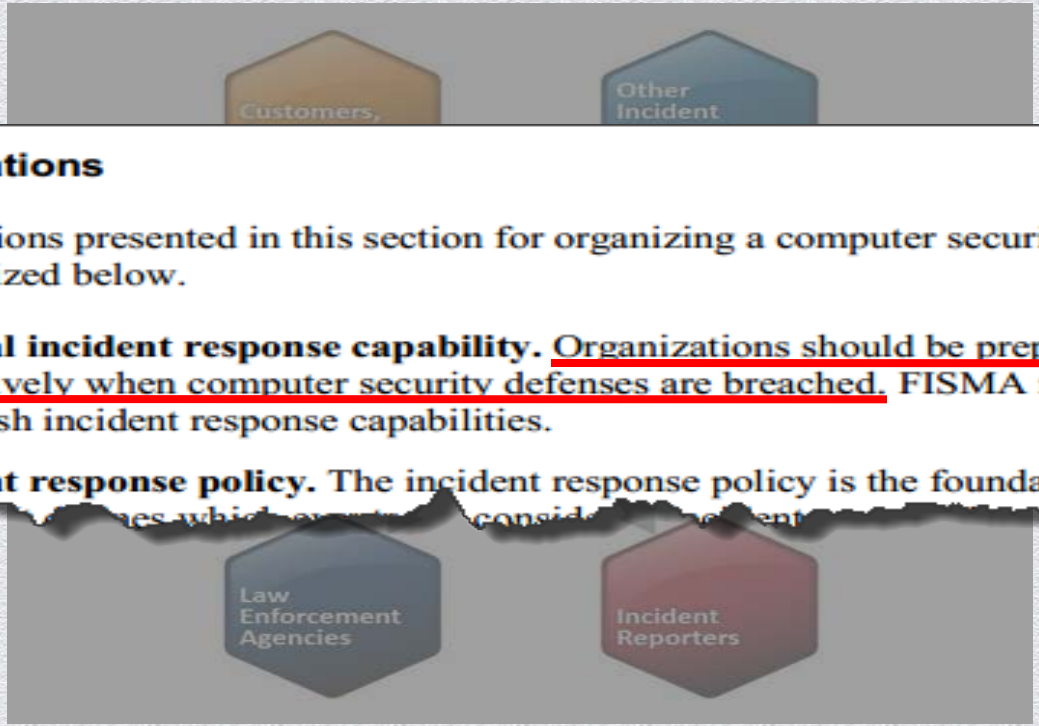
Blackstone

#RSAC

RSACONFERENCE2014

Pages 7-18: Incident Response Plan

Pages 7-18: Incident Response Plan



2.6 Recommendations

The key recommendations presented in this section for organizing a computer security incident handling capability are summarized below.

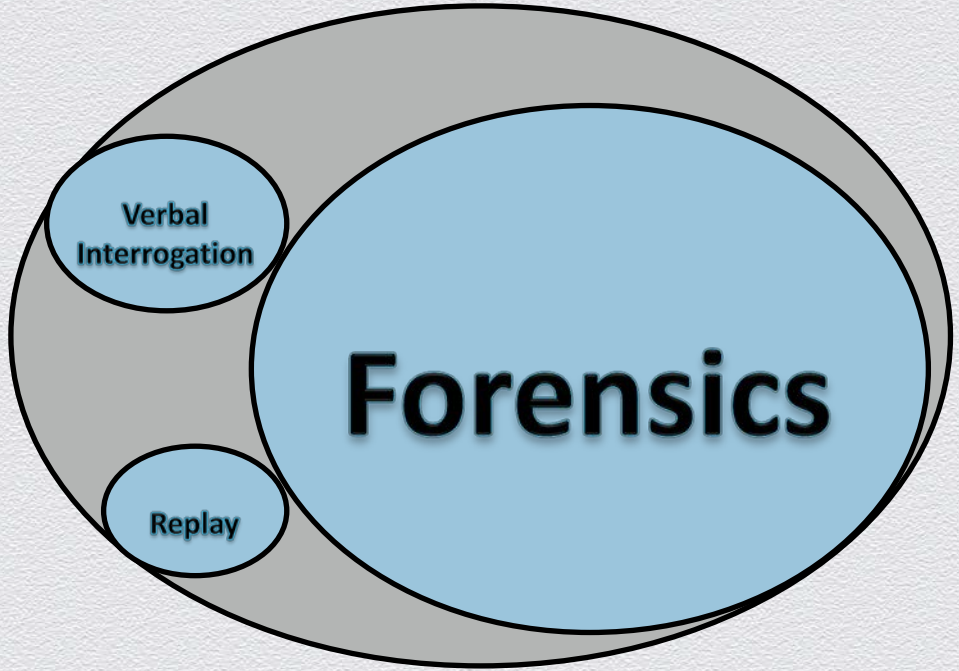
- **Establish a formal incident response capability.** Organizations should be prepared to respond quickly and effectively when computer security defenses are breached. FISMA requires Federal agencies to establish incident response capabilities.
- **Create an incident response policy.** The incident response policy is the foundation of the incident

Blackstone

#RSAC

RSACONFERENCE2014

Forensics is a key component of incident response often overlooked

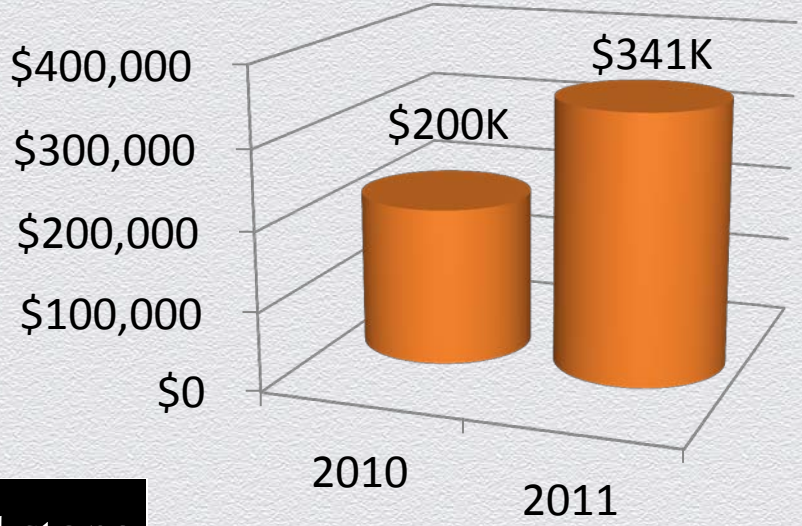


NetDiligence
Cyber Risk Assessment & Data Breach Services

Cyber Liability & Data Breach Insurance Claims

A Study of Actual Payouts for Covered Data Breaches

Response / Forensics Costs per Breach



- Data Breaches currently require experts to figure out what happened with limited visibility and resources
- Response Costs increased by 75% from 2010 to 2011 ($200k → $341k)
- Likely due to an increase in attack sophistication, ease of attack new regulatory requirements, and shortage of skilled experts and solutions

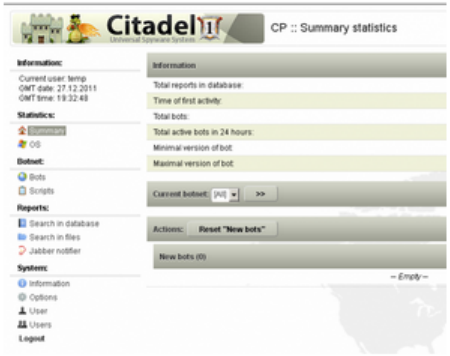
Blackstone

‘Citadel’ Trojan Touts Trouble-Ticket System

133 tweets
TOP ★5K
retweet

Underground hacker forums are full of complaints from users angry that a developer of some popular banking Trojan or bot program has stopped supporting his product, stranding buyers with buggy botnets. Now, the proprietors of a new **ZeuS Trojan** variant are marketing their malware as a social network that lets customers file bug reports, suggest and vote on new features in upcoming versions, and track trouble tickets that can be worked on by the developers and fellow users alike.

The ZeuS offshoot, dubbed **Citadel** and advertised on several members-only hacker forums, is another software-as-a-service malware development. Its target audience? Those frustrated with virus writers who decide that coding their next creation is more lucrative and interesting than supporting current clients.



“Its no secret that the products in our field — without support from the developers — result in a piece of junk on your hard drive.

Blackstone

#RSAC
RSACONFERENCE2014

133 Underground hacker forums are full of complaints from users angry that a developer

The basic Citadel package — a bot builder and botnet administration panel — retails for $2,399 + a $125 monthly "rent," but some of its most innovative features are sold as a la carte add-ons. Among those is a $395 software module that allows botmasters to sign up for a service which automatically updates the bot malware to evade the last antivirus signatures. The updates are deployed via a separate Jabber instant message bot, and each update costs an extra $15.

creation is more lucrative and interesting than supporting current clients.

"Its no secret that the products in our field — without support from the developers — result in a piece of junk on your hard drive.

Breach	Attacker Cost	Defender Cost
0	$2,795	$0
1	$2,935	$200,000
2	$3,075	$400,000
3	$3,215	$600,000
4	$3,355	$800,000
5	$3,495	$1,000,000

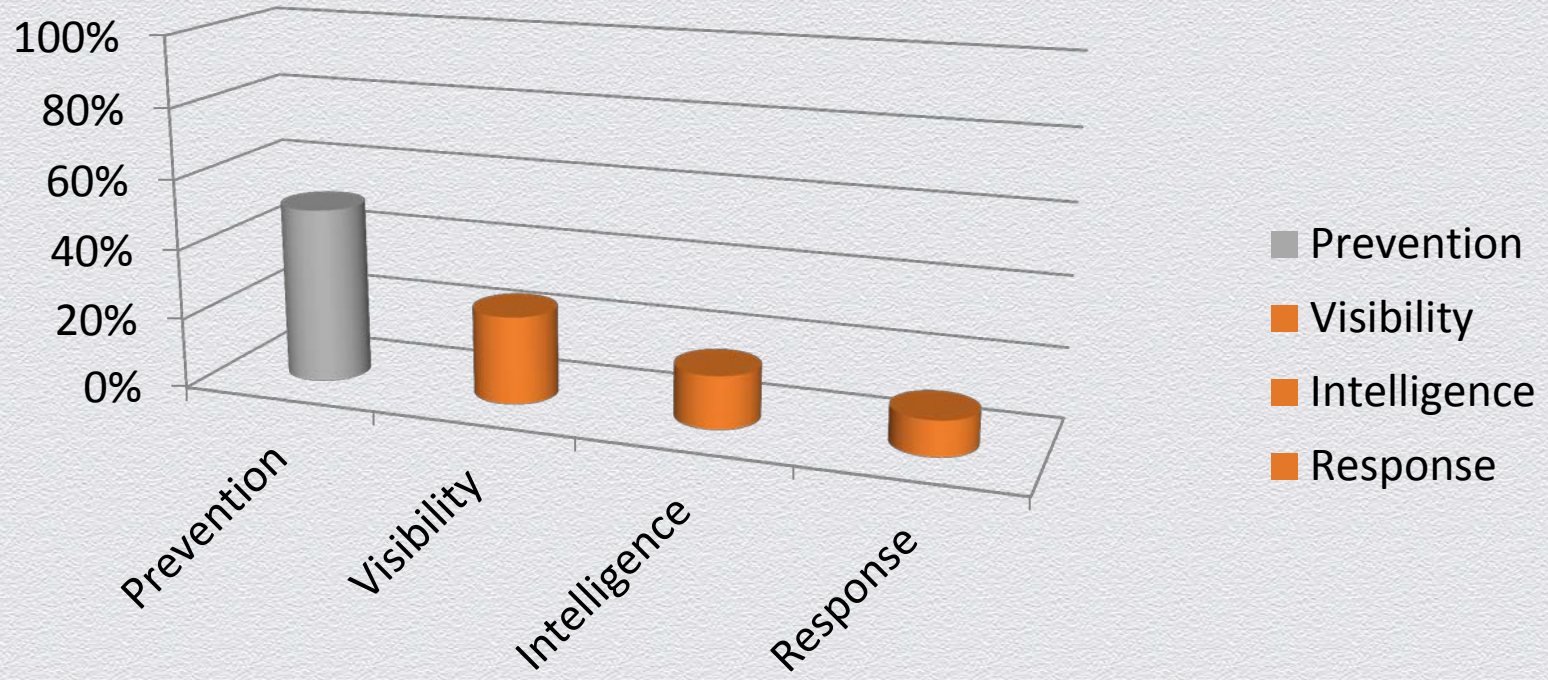
Breach	Attacker Cost	Defender Cost
0	$2,795	$0
1	$2,935	$200,000
2	$3,075	$400,000
3	$3,215	$600,000
4	$3,355	$800,000
5	$3,495	$1,000,000
2416	$341,035	$281,800,000

Cost to respond in 2011 = $341K

Blackstone

This Is Simply Not Sustainable

Change #3: Adjusted enterprise resource allocation



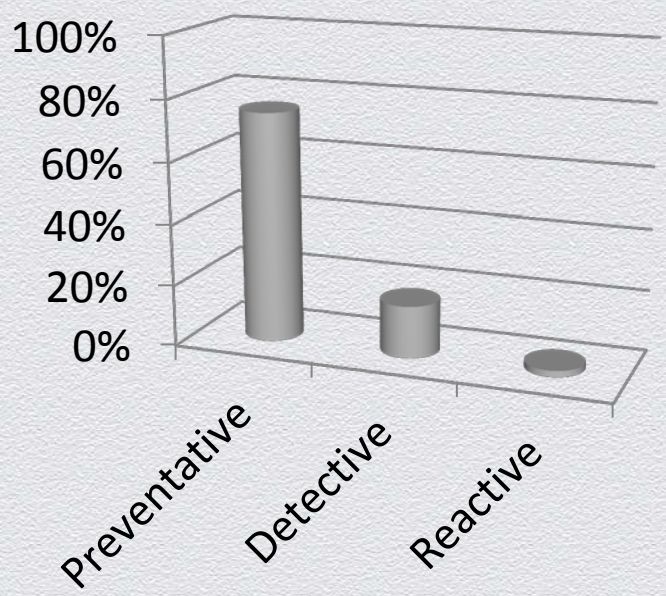
Blackstone

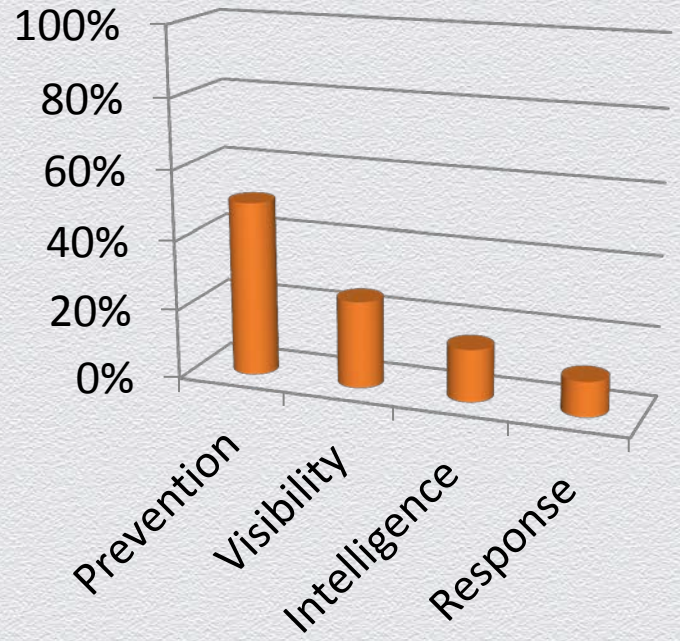
#RSAC

RSACONFERENCE2014

Bringing It All Together

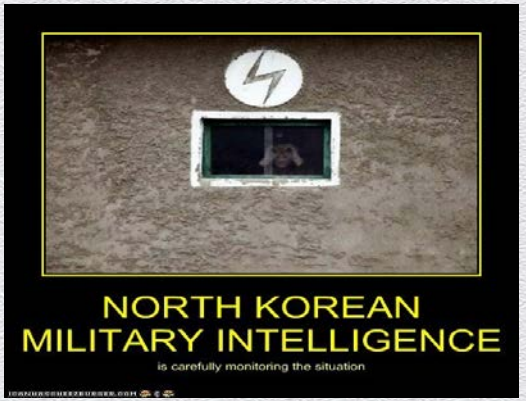
Call To Action: Shift resources and focus, and change our approach





Examples of responding to this Call To Action

- **Visibility**
  - Detailed awareness of what is happening on the network and the host in real-time
  - Close collaboration with development, infrastructure and networking teams (e.g. Solarwinds)



- **Intelligence**
  - Tuning defenses based on adversary actions and attack profiles
  - Risk-based intelligence patching for flaws commonly exploited by cyber espionage and cyber crime
- **Response**
  - Workstation / laptop build methodology (e.g. offline files)
  - Automated integration of alerts for response / forensics in minutes down to the host level

- Improve our visibility
- Acquire more intelligence
  - Understand what is happening in the world around you
  - Understand your adversary
- Shift from reactive to planned response
- Don’t let the market drive your program

Blackstone