RSAConference2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: **LAB4-W03**

Incident Preparedness Report: Taming the Data Beast

Chris Novak
Director
Global
VTRAC

John Grim
Managing Principal
Americas
VTRAC

K. Eric Gentry
Managing Principal
RRR
VTRAC

Ashish Thapar
Managing Principal
APJ
VTRAC

verizon business ready

#RSAC

Proprietary Statement

This document and any attached materials are the sole property of Verizon and are not to be used by you other than to evaluate Verizon's service. This document and any attached materials are not to be disseminated, distributed, or otherwise conveyed throughout your organization to employees without a need for this information or to any third parties without the express written permission of Verizon.

The VTRAC Team

Lead Investigator
Endpoint Forensics Examiner
Malware Reverse Engineer
Network Forensics Specialist
Threat Intelligence Analyst
PFI Investigator

First-Hand Experience

- VTRAC = Verizon Threat Research Advisory Center
- Investigations for hundreds of global commercial enterprises and government agencies annually
- Cyber intelligence, endpoint forensics, network forensics, threat hunting, malware reverse engineering
- Annual DBIR and its companion—the Data Breach Digest

Incident Preparedness Report – Taming the Data Beast

What if the next data breach beast reared its ugly head and appeared in your camp? Moreover, key stakeholders are still in denial that a data breach could, let alone did, happen.

Over the years, our caseload continues to supports our observation that data breach scenarios are not so much about threat actors, or even about exploited vulnerabilities, but are more about the situations in which IR stakeholders find themselves.

We'll look to put this session's attendees in the shoes of incident responders seeking to improve breach response efforts and mitigate future cybersecurity incidents.

As we move through each 'phase', we'll highlight crucial situational pivot points as experienced in our investigative response casework and seen through trending metrics in our IR Capability Assessment and Data Breach Simulation observations.

Finally, we'll end the session by re-capping, what is in our experience, the 10 incident response elements to tame the data beast.

1 – Credential Theft – the Monster Cache

- Industry frequently targeted by espionage-oriented threat actors via phishing emails as entry vector
- +500 corporate user creds dumped and available in DarkNet forum
- Transfer logs, phishing email, and threat intel uncovered source and provided threat actor context
- Activity stemmed from compromised account with phishing emails sent to internal end users
- Email included link to credential-harvesting site, prompting users to authenticate with creds

http://www.verizonenterprise.com/resources/

1 – Credential Theft – the Monster Cache

Countermeasures

http://www.verizonenterprise.com/resources/

Mitigation and Prevention

- ✓ Keep current on the cyber threat landscape and threat actions targeting your industry
- ✓ Integrate threat intelligence into operations and facilitate threat data dissemination
- ✓ Implement Multi-Factor Authentication (MFA)

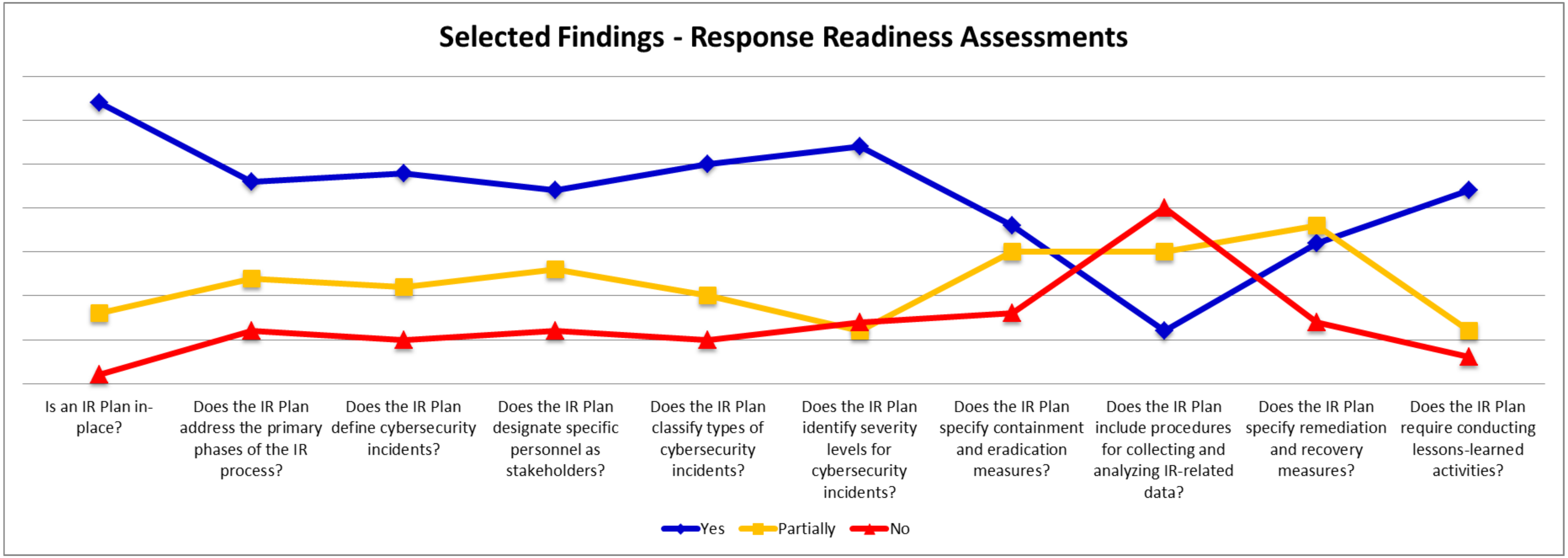
Detection and Response

- ✓ Review logs to learn how threat actors are targeting your organization
- ✓ Consider creating honeypots to detect, counteract, and gain insight into targeted attacks
- ✓ Upon being notified of user credential compromise, change them immediately!

Incident Preparedness Report

SNEAK PEEK

- Selected Findings – Incident Response Readiness Assessments



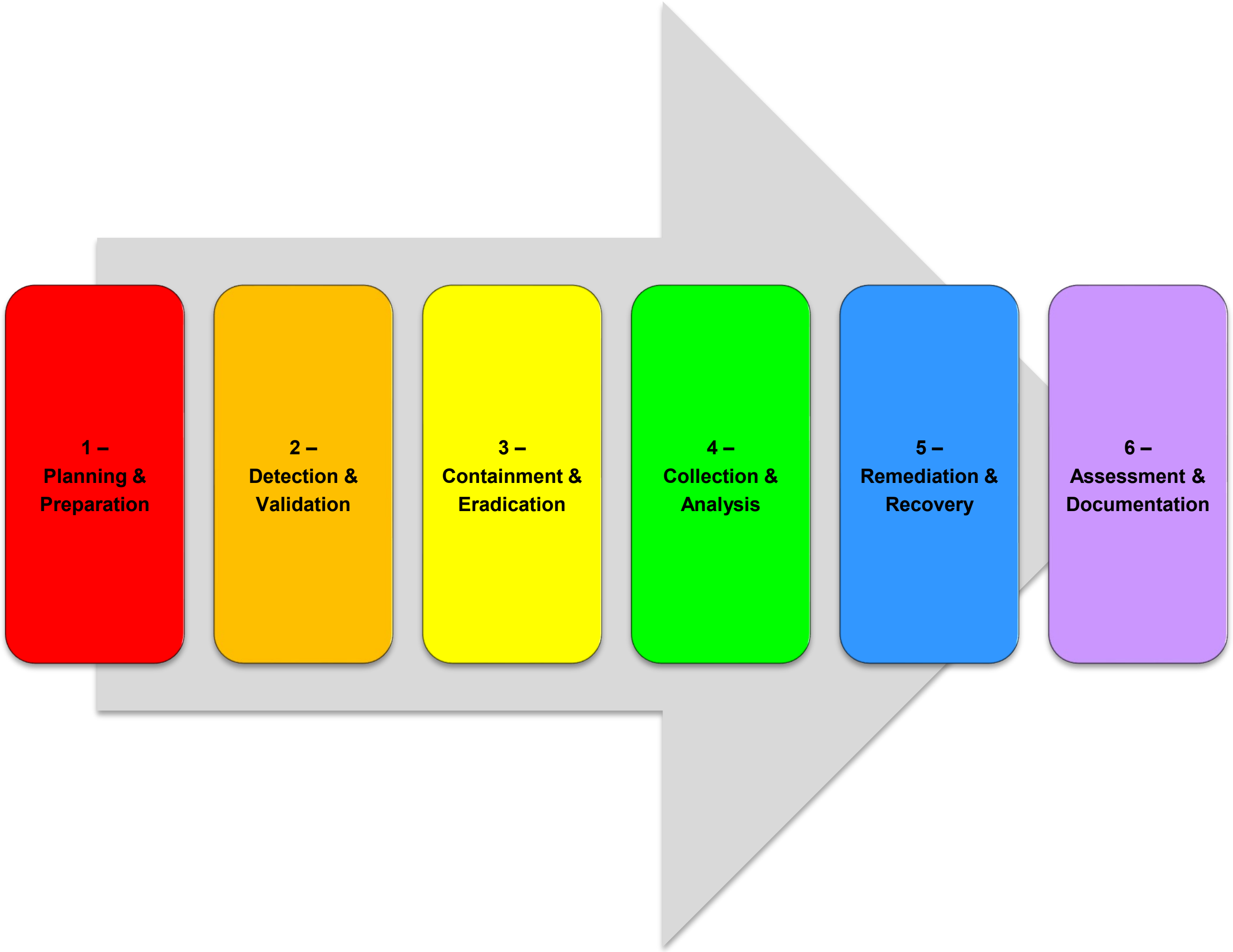
Learning Lab - Exercise Setup

Group	Table	Scenario
1	1-3	2, 8
2	4-6	3, 17
3	7-9	4, 10
4	10-12	7, 18

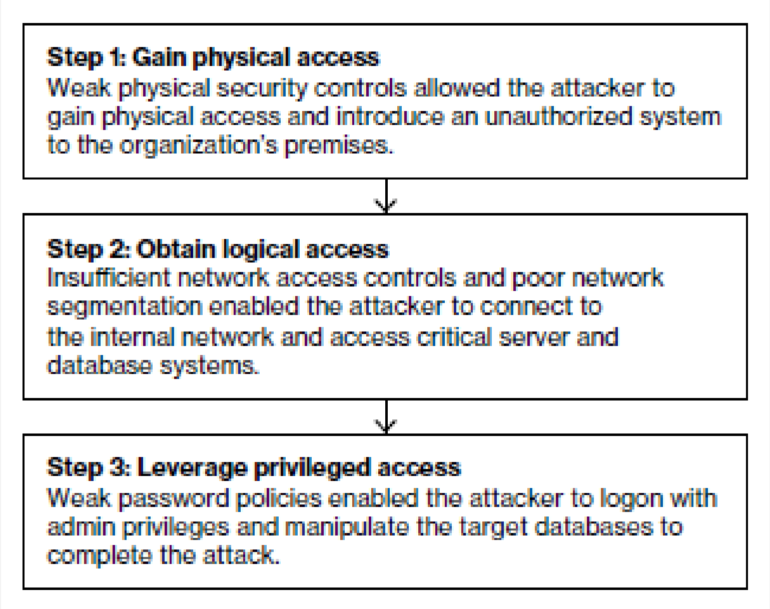
- Think, Communicate and Collaborate
- Make full use of the available resources (e.g. flip charts)
- Keep sound levels low so others can discuss
- Each team gets 15 minutes to discuss
- Each team gets 5 minutes to present their countermeasures

Incident Preparedness Strategy

- What preparatory actions could have been taken?
- What activities would be important to detect and triage the incident?
- How would this incident be contained, the threat eradicated, and the situation be recovered?
- What steps could be taken to prevent / mitigate this incident?


1 – Planning & Preparation
2 – Detection & Validation
3 – Containment & Eradication
4 – Collection & Analysis
5 – Remediation & Recovery
6 – Assessment & Documentation

2 – Insider Threat – the Card Shark



Step 1: Gain physical access
Weak physical security controls allowed the attacker to gain physical access and introduce an unauthorized system to the organization's premises.

Step 2: Obtain logical access
Insufficient network access controls and poor network segmentation enabled the attacker to connect to the internal network and access critical server and database systems.

Step 3: Leverage privileged access
Weak password policies enabled the attacker to logon with admin privileges and manipulate the target databases to complete the attack.

http://www.verizonenterprise.com/resources/

- Initial SIEM log analysis identified suspect system within victim environment
- Unknown system accessed critical PCI server database / conducted unauthorized ATM withdrawals
- Connected devices full network access, monitoring incorrectly configured, SIEM alerts unheeded
- No identification verification, no ACLs, no one consistently at security desk
- Unchanged / easily guessable passwords, admin privs for database accounts

8 – eCommerce Breach – the Flutterby Effect

- Several ecommerce customers experienced 'frozen pages' when checking out online
- Development environment tests found no issues; production environment tests resulted in frozen page
- Web page production-development comparisons revealed malcode inserted into production page
- Examination revealed attacker gained access to payment processing app and inserted code
- Payment card data redirected to remote domain; malcode failed to execute causing browser to hang

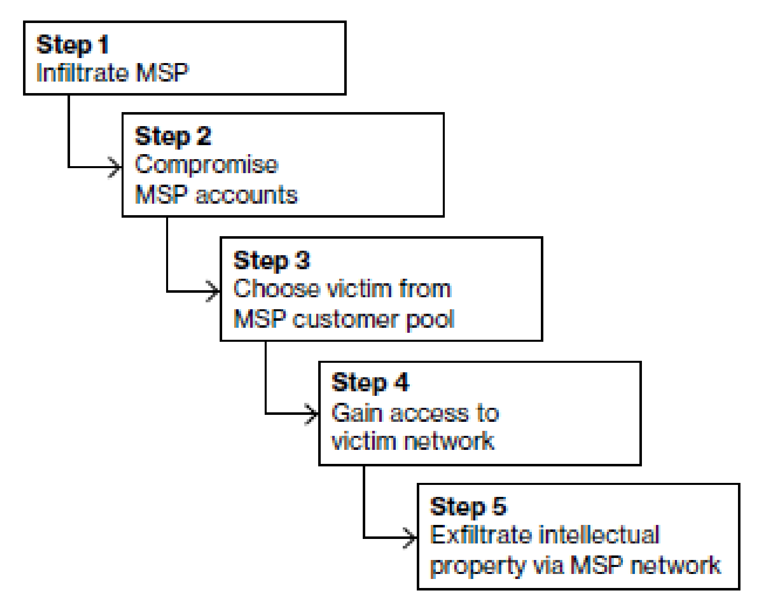
http://www.verizonenterprise.com/resources/

3 – Crypto-Jacking – the Peeled Onion

- Victim observed several firewall alerts on blocked suspicious outbound traffic to Tor network
- Network FPCs and memdump exam identified other potentially compromised systems
- Network connection review revealed connections to Tor network and Monero cryptocurrency mining pool
- Malicious network activity also found originating from Microsoft PowerShell process running on systems
- Network forensics confirmed ransomware-like malware propagation
- System exam confirmed Windows SMB Remote Code Execution Vulnerability unpatched

http://www.verizonenterprise.com/resources/

17 – Cloud Storming – the Slivered Lining



Step 1
Infiltrate MSP

Step 2
Compromise MSP accounts

Step 3
Choose victim from MSP customer pool

Step 4
Gain access to victim network

Step 5
Exfiltrate intellectual property via MSP network

http://www.verizonenterprise.com/resources/

- LE notified victim of systems likely compromised due to connections with malicious IP address
- Network log review found two systems making connections; both systems contained intellectual property
- Investigation yielded active RAT; malware analysis revealed domain names resolving to malicious IP address
- Intel found RAT was associated with APT10; threat actor associated with intellectual property theft and MSP breaches
- IoC scans found multiple systems infected with backdoor persistence tools and various compromised accounts
- Investigation determined MSP accounts leveraged for network access; dark web monitored following investigation

4 – Cyber-Espionage – the Katz-Skratch Fever

- LE notified victim that several foreign IP addresses were communicating with systems
- In-scope system examination revealed 'mimikatz', a clear text password and NTLM hash scraping tool
- Sys admin with engineering division domain controller access phished with email / PDF malicious attachment
- With sys admin credentials, threat actor moved laterally across domain controllers and engineering file servers
- Uploaded approx. 3,000 sensitive, proprietary CAD drawings, schematics, and designs to FTP site

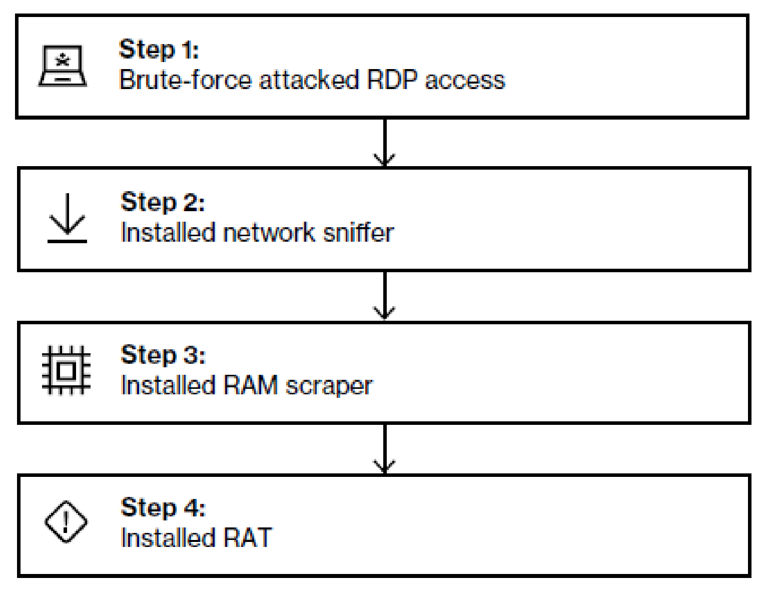
http://www.verizonenterprise.com/resources/

10 – ICS Attack – the Eclectic Slide

Countermeasures

- LE notified victim SOC of possible compromise; information was 'TLP Red' (public sharing prohibited)
- Spear phishing attack occurred against energy sector; targeted recipients were executives and lead engineers
- Email examination found Word document hosted on internet; communicated with C2 server
- When opened, document searched via SMB protocol for specific, malicious template on threat actor server
- Once downloaded, malicious template via macros spawned PowerShell instance to steal credentials
- Threat actor targeted recipients based on public profiles on social networking sites

7 – PoS Intrusion – the Faux PoS



Step 1:
Brute-force attacked RDP access

Step 2:
Installed network sniffer

Step 3:
Installed RAM scraper

Step 4:
Installed RAT

Figure 2. Third-party server attack stream

http://www.verizonenterprise.com/resources/

- Through CPP analysis, acquiring banks suspected PCI breach; millions of dollars fraudulent transactions occurred worldwide
- Evidence included transaction flow, CPP analysis data, third-party access; store PoS systems, business unit systems, and several third-party servers
- Forensic artifacts lost as vendor restarted systems, executed AV scans, changed passwords, deleted accounts / logs
- Investigation found PoS servers with unrestricted internet ingress, unknown RDP logins, backdoor RAT, RAM scraper, network sniffer, as well as 100,000+ clear text transaction log entries on third-party server
- Recovery included rebuilding systems, restricting RDP access with source address filtering, requiring MFA for remote logins, reviewing third-party service provider security controls

18 – Web App Attack – the Tuple-Row Honey

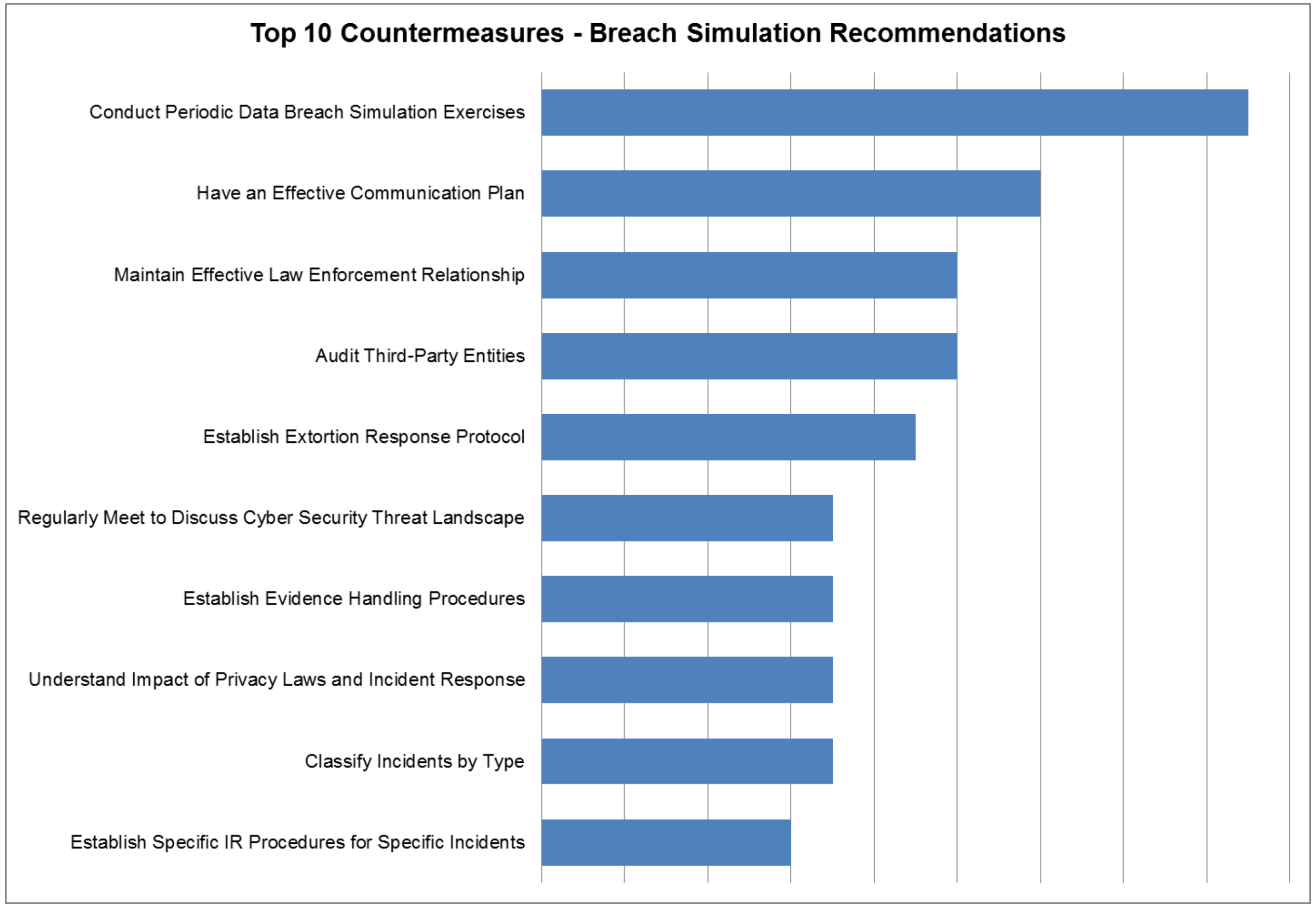
- Victim hosted online 'hackathon' event to identify quality candidates; web app designed for online registration
- Hackathon enormous success; however, significant traffic accessed web app server; several AV alerts
- Initial investigation determined attacker exploited RCE web server vulnerability; WAF not in place
- Attacker leveraged web shells for remote access prior to AV alerts
- Logs found successful database queries on job candidate database; attacker plundered candidate PII

http://www.verizonenterprise.com/resources/

Incident Preparedness Report

Top 10 Countermeasures – Breach Simulation Recommendations

SNEAK PEEK



Take Aways

10 Key Incident Response Elements

- ✓ Governance & Standards
- ✓ Incident Response Stakeholders
- ✓ IR Process Flow
- ✓ Detection & Validation Sources
- ✓ Incident Classification
- ✓ Escalation & Communication
- ✓ Tactical IR Team
- ✓ Pre-Designated Reactive Measures
- ✓ Post-Mortem Lessons-Learned
- ✓ Key Performance Indicators

Take Aways

Applying What You Learned Today

Next Week

- ✓ Review the Verizon DBIR and DBD (http://verizonenterprise.com/dbir)
- ✓ Familiarize yourself with the VERIS Framework (http://veriscommunity.net)

Within Three Months

- ✓ Socialize the VERIS Framework with your IR stakeholders
- ✓ Hold your first data breach simulation exercise (featuring a relevant DBD scenario) to identify any gaps
- ✓ Update your IR Plan; train your First Responders

Within Six Months

- ✓ Hold your second data breach simulation exercise to validate your IR plan and capabilities