Breach simulation scenario #2

Insider threat – The card shark

verizon

Using the breach simulation kits.

This is part two in a series of five data breach scenarios we're using to illustrate the need for an IR Plan, playbooks and their underlying components. These scenarios, together with the countermeasure worksheet and solutions, form Breach Simulation Kits (BSKs). BSKs can facilitate data breach simulation workshops involving internal IR stakeholders and tactical responders, as well as external entities. Conducting a BSK workshop session is a five-step process.

Step 1 – Getting started

To facilitate a BSK workshop, you'll need:

- A suitable facility – a "war room" or conference room free of noise and other distractions
- A whiteboard or butcher-block paper and markers
- Printouts of scenarios and countermeasures worksheets (and highlighters) for each participant

A typical BSK workshop session consists of 1-2 scenarios and can last for 1-2 hours, depending on participant knowledge levels and experience.

Step 2 – The scenario

Begin the workshop by distributing printouts of the scenario (including situation, response and lessons learned) to participants (optional: distribute the countermeasure worksheet).

Cyber-espionage – The "katz-skratch fever"	Notes
The situation While espionage has existed for thousands of years, cyber-espionage (threat actors targeting sensitive or proprietary data on digital systems) is still a relatively new concept. Recently, a manufacturing customer engaged the VTRAC | Investigative Response Team to let us know they'd been contacted by law enforcement regarding a possible data breach. The Chief Information Security Officer (CISO) had been notified of several foreign IP addresses that may have been communicating with systems inside his environment. The CISO requested we immediately report to headquarters to begin investigation into the suspicious IP addresses.	Contact digital forensics firm Maintain effective law enforcement contacts Check security information and event management (SIEM) events

Figure A: The scenario – The situation, response and lessons learned

Give participants 10-15 minutes to read the scenario, highlight and take notes. Allow participants to talk and discuss among themselves.

Step 3 – Countermeasure worksheet

After participants have read the scenarios, facilitate a discussion by selecting a participant to walk through the situation, response and lessons learned. Discuss key observations on countermeasures. Take notes on the whiteboard or butcher-block paper (or use the countermeasures worksheet) by progressing through the six phases of incident response (include prevention and mitigation countermeasures).

Phase	Countermeasure
1 – Planning and Preparation	• Create an IR playbook for cryptocurrency-related scenarios; train incident responders on efficient and effective response activities
2 – Detection and Validation	• Conduct periodic threat hunting activities across the network to locate and identify any undetected cyber threat activity evading traditional cybersecurity tools • Be vigilant for anomalous activity, such as sharp increases in system CPU usage or network egress/ingress traffic volumes; monitor firewall and network appliance logs for anomalous activity

Figure B: Countermeasure worksheet – the six phases of incident response plus mitigation and prevention

Give the participants 15-20 minutes to discuss, and be sure everyone has an opportunity to speak.

Step 4 – Countermeasure solutions

Distribute countermeasure solutions (answers). Continue facilitating the discussion by comparing participant solutions to countermeasure solutions. Do they differ? Did the participants come up with more actionable items than those provided in the countermeasure solutions?

Detection and response

- If not already involved, engage law enforcement when the time is right, and third-party investigators when applicable
- Collect access logs to key servers and email; prior to system shutdown, collect in-scope volatile data and system images; examine quickly
- Utilize internal and external intelligence resources to develop actionable intelligence on threat actor modus operandi and indicators of compromise (IoCs)

Mitigation and prevention

- Provide, at least annually, user cybersecurity awareness training, emphasizing awareness and reporting suspicious emails
- Make external emails stand out; prepend markers to the "Subject:" line indicating externally originated emails
- Move beyond single-factor authentication and implement multifactor authentication; require virtual private network (VPN) access for remote connections to the corporate environment

Figure C: Countermeasure solutions

Give the participants 10-15 minutes to discuss.

Step 5 – Lessons learned

Complete the session by conducting a lessons-learned discussion, noting participant feedback (e.g., what went well, what went less smoothly and what can be improved on in the next session). Assemble feedback and countermeasure solutions in an action plan to update the IR Plan, determine additional IR resource requirements, and identify internal IR stakeholder and tactical responder training needs.

Give participants 10-15 minutes to discuss.

Insider threat – The card shark[1]

The situation

While most attacks come from outside sources such as hacking or spear phishing, we occasionally see attacks coming from within a victim organization's own network environment.

One case involved payment card data compromise, with unauthorized automated teller machine (ATM) withdrawals that resulted in significant financial loss. The VTRAC | investigative response team was engaged to conduct a payment card industry (PCI) forensic investigation.

Investigative response

After arriving onsite, we were granted immediate access with no security or identification checks. This was unexpected and unusual, considering the circumstances. We were also informed that most of the staff we wanted to interview had been replaced, and that new hires were still getting familiar with the environment.

Our initial security information and event management (SIEM) log analysis identified a malicious system in the environment. This system was neither corporate-owned nor "known," raising multiple questions such as how the system made its way onto the network, where it was located, how it gained access into the PCI environment and why no one noticed the initial alerts.

All we had to go on was that a rogue system connected to the network, and indications that it had accessed critical PCI server databases and conducted unauthorized withdrawals. We still didn't know how the system came to be on the network or exactly how the attack occurred, so we focused on gathering more information.

We conducted interviews and collected technical information, such as the network topology, to fully scope the incident and identify possible intrusion vectors. This process revealed that the entire network structure was flawed from the ground up.

Despite a few internal firewalls, the network was essentially flat. In addition, full network access was available to any connected device due to the lack of even rudimentary access controls. In-place network monitoring was misconfigured, and while there was a SIEM in place, no one was reviewing and investigating alerts.

Notes:

[1]https://enterprise.verizon.com/resources/casestudies/2018/data-breach-digest-2018-the-card-shark.pdf

These fundamental design flaws across the network were an open door for attack—and made it trivial for a threat actor to fly under the proverbial radar.

We reviewed physical security controls at the location where the attacker's system connected during the attack. The location was a main data center, a large office building with a publicly accessible area.

To our surprise, the data center's access was secured with just a standard keyed door. Once inside, all offices were easily accessible. This lax security posture included no ID verification, no access control lists, and no one consistently occupying security desks. We quickly realized that accessing employee areas from public areas would be relatively easy due to weak physical security.

We also identified major flaws in the organization's digital security posture. These included easily guessable passwords, unchanged administrator account passwords, shared user and admin accounts, database access by default user accounts, and administrator privileges for every database user account.

Forensic analysis revealed an attacker with physical access used this suspect system to connect to an application server via an administrator account. The attacker generated scripts to manipulate the database, executing these on the night of the incident. Unfortunately, the suspect system was never found and was not available for analysis.

Lessons learned

In the end, it was obvious what led to the compromise:

- **Step 1:** Gain physical access. Weak physical security controls allowed the attacker to introduce an unauthorized system into 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 log on with admin privileges and manipulate the target databases to complete the attack.

Finally, lack of proper network monitoring prevented the organization from detecting the attacker at an early stage. At the end of this investigation, it remained unknown whether the attacker had insider support. Potential answers to many questions vanished with the undiscovered suspected system.

Notes:

Countermeasure solutions

Detection and response

- Properly configure network security monitoring software (e.g., SIEM, Intrusion Detection System (IDS)) based on use cases; regularly review outputs and events
- Train employees on cybersecurity policies and procedures, and sensitize them to report suspicious cybersecurity and physical security incidents; conduct periodic mock incident tabletop exercises to test responders and stakeholders
- Include an IR playbook within the IR Plan; hold After Action Reviews (AARs) after incidents and capture lessons learned for future improvements
- Proactively assess for payment card fraud; contact acquirers and card brands; conduct internal checks and audits (cover all 12 PCI DSS requirements); engage law enforcement when the time is right

Mitigation and prevention

- Restrict physical access: Employ physical security measures such as identity cards, card swipes and turnstiles; further restrict access to sensitive areas; monitor via closed-circuit camera system; prohibit personal devices on the network
- Restrict logical access: Segment the network; prevent rogue system connection to the network; implement multi-factor authentication (MFA); use complex passwords for all user accounts; apply the principle of least privilege for access to sensitive data

Countermeasure worksheet

Workshop participants can enter their discussion notes on breach countermeasures here.

Phase	Countermeasure
1. Planning and preparation	
2. Detection and validation	
3. Containment and eradication	
4. Collection and analysis	
5. Remediation and recovery	
6. Assessment and adjustment	
0. Mitigation and prevention	

Table 4 - Breach simulation countermeasure worksheet

Data breach and cybersecurity resources

https://enterprise.verizon.com/resources/

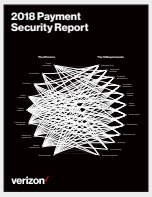
2019 Incident Preparedness and Response Report: Taming the data ~~beast~~ breach.

2019 Data Breach Investigations Report

2019 Insider Threat Report: Out of sight should never be out of mind.

2019 Mobile Security Index: It's time to tackle mobile security.

2018 Data Breach Digest (18 scenarios)



2018 Payment Security Report

2019 CISO's Guide to Cloud Security: What to know and what to ask before you buy.

5 Considerations for Evaluating a Modern Enterprise Security Platform.

For the Verizon Incident Preparedness and Response report, executive summary and additional scenarios, visit
enterprise.verizon.com/resources/reports/vipr/

verizon