RSAConference2020

Learning Labs

HUMAN ELEMENT

Only After Disaster Can We Be Resurrected: Field Lessons in Cyber-Incidents

Post-event Write-up

Mark Sangster
VP and Industry Security Strategist
eSentire

Jon Washburn
Chief Information Security Officer (CISO)
Stoel Rives LLP

Table of Contents

The Lab

What we reviewed

This workshop used investigations, air crashes and nuclear accidents to expose specific biases that hinder our ability to avoid casting blame, and often hide the systemic issues that truly led to the disaster. Attendees received hands-on experience with four real-life cyber-incidents and are exposed to the chaotic, volatile atmosphere permeating these events.

For those of you that attended, we hope your group exercises generated new ideas about how to approach various breach, attack and disaster scenarios, from a full incident-management perspective involving communications, reputational risk, business impact and other factor besides just technical considerations.

Key Considerations

We recommend you follow up with your organizations on these key elements discussed during the workshop exercises:

- Incident Response Plans
  - Regular review
  - Tabletop exercises
  - Cover life safety/environmental threats as well as technical/operational threats
- Incident Management Teams
  - Membership
  - Have a plan for running the team
  - Regular meetings and tabletops
- Business Impact Assessments (BIAs)
  - Understand the impact to core functions
  - Understand IT dependencies
  - Can you still function with long-term impacts to resources?
- Business Continuity Plans (BCPs)
  - Understand the impact to core functions
  - Understand IT dependencies
  - Can you still function with long-term impacts to resources?
- Risk Management
  - Document a formal policy and plan
  - Assessing risk: Qualitative v. Quantitative (or both)
  - Maintaining a Risk Register
  - The four risk treatment options
    - Accept
    - Avoid
    - Transfer
    - Mitigate
  - Obtaining sponsorship from management and sign-off on the risk
  - Accountability/Ownership of risk
  - Identifying Key Risk Indicators (KRI)
  - Measuring Key Performance Indicators (KPI) – how do you know you're managing risk effectively?

Lab Materials

In the event you did keep the paper handouts, included are the materials from this lab session, which are yours to use internally within your organization if desired:

- Probability Table
- Impact Table
- Heat Map
- Tabletop Exercises

As noted in the Lab, these exercises, while modeled after actual events across multiple real-world scenarios, are entirely fictional.

Probability Table

10	Incident	*Risk event has been realized/is actively occurring* and is related to a specific incident.
9	Live	*Risk event has been realized* but has not yet resulted in a specific incident.
8	Frequent/A critical process that should be frequently occurring is not occurring	*Occurs frequently*, or has not occurred but *is expected to manifest in the near future*
7	Ongoing/An important process that should be occurring is not occurring	*Occurs fairly regularly* or has not occurred but *has a high probability of occurring.*
6	Likely/A critical process that should be periodically occurring is not occurring	*Has occurred a few times* or has not occurred but *has a likely probability of occurring.*
5	Occasional/Ad Hoc/An important process that should be periodically occurring is not occurring/Important documentation is missing	*Has occurred as a one-time incident* or has not occurred but *has a somewhat likely probability of occurring.*
4	Rare	*Has occurred as a one-time incident* or has not occurred but *has a reasonable probability of occurring.*
3	Probable	Could happen, but not expected to occur.
2	Possible	Could happen, but only under specific circumstances, not expected to occur.
1	Unlikely	Could happen, but only under very specific circumstances that are not likely to occur.
0	Mitigated	Risk has been closed in the Register

Impact Table

10	Emergency	Immediate response required, potential to halt critical operations. Unlikely to control or counteract if realized, response could require unachievable time/financial cost commitment.
9	Critical	Critical systems or processes affected, disruptive to critical business operations. Challenging to control or counteract if realized, response would require very high time/financial cost commitment.
8	Core systems	Core systems or processes affected, disruptive to core business operations. Difficult to control or counteract if realized, response could require very high time/financial cost commitment.
7	High	Important systems or processes affected, disruptive to necessary business operations. Costly to control or counteract if realized, response would require high time/financial cost commitment.
6	Significant	Important systems or processes affected, somewhat disruptive to necessary business operations. Significant effort to control or counteract if realized, response could require significant time/financial cost commitment. A significant impact is expected due to the lack of an important leadership role, point of contact and/or defined process.
5	Moderate	Regularly used systems or processes affected OR specific process affected with no workaround, may be disruptive to business operations. Moderate effort to control or counteract if realized, response would require time/financial cost commitment.
4	Negative impact to systems, process or function	Popular systems or processes affected, can be worked around OR specific system or process affected with no workaround. Would require effort from more than one group to control or counteract if realized, response could require time/financial cost commitment. Lack of an important leadership role, point of contact and/or documented process has the potential to negatively impact a specific system or function.
3	Specific non-core systems	Specific system or process affected, can be worked around. Would require effort from one group to control or counteract if realized, response would require some time/financial cost commitment.

2	Low	Specific system or process affected, can be easily worked around. Would require some effort to control or counteract if realized, response would require a low time/financial cost commitment.
1	Very Low	Specific system or process affected, can be easily worked around. Would require minimal effort to control or counteract if realized, response would require a low time/financial cost commitment.
0	Mitigated	Risk has been closed in the Register

Heat Map

PROBABILITY/IMPACT HEAT MAP											
Impact	Likelihood										
	10	9	8	7	6	5	4	3	2	1	0
10											
9											
8											
7											
6											
5											
4											
3											
2											
1											

Low Risk – Green
Moderate-Low Risk – Blue
Moderate Risk – Orange
Moderate-High Risk – Dark Orange
High – Red
Critical Risk – Dark Red

Tabletop Exercise 1 – Emotet Attack Scenario

Jane, the Help Desk Manager at OMG Health Care woke up this morning to an alert that her antivirus software quarantined a new variant of Emotet, a well-known malware worm that is generally the precursor to the Emotet/Trickbot/Ryuk "triple threat" attack. Since the threat was "quarantined" she breathed a sigh of relief and went back to sleep.

While on her way to work, Doctor Goode forwarded Jane an email from Mike at Health Care Clearinghouse stating that they received a "spoof" phishing email with a malicious attachment from "Doctor Goode" <fakeemail@alol.com> with the subject "Billing issues for patient John Smith."

After arriving at her desk, Jane is told that a night nurse reported receiving an email titled "Re: re: List of dishes for Friday's Potluck" that appeared to be from an internal email thread, with an attachment she hadn't seen before called "List.docx." When she opened the attachment, she saw a couple weird windows appear and disappear. Jane can see the email was sent from "Paul Jones, RN" <anotherfake@yahoo!.com>).

PART I:

THE INVESTIGATION

- In the email example, it is clearly apparent that the scam account that sent the spoofed email includes the message body of a private message that was sent from Doctor Goode's OMG email account to Mike from back in September.
- Jane calls her MSSP and they help her dig into the AV system and review the logs, where they discover 22 computers were cleaned – Doctor Goode's was one of them. They find that it took the AV solution almost 20 hours to detect and quarantine this new Emotet variant (the variant initially installed but wasn't quarantined/removed until the PCs received/auto-installed the latest definitions update.)

CONTEXT

- OMG has an EMR system but isn't good about using it.
- OMG has yet to roll out 2FA for remote access.

What should Jane and her MSSP do next?

What is the potential impact?

Who does OMG likely have to notify, and why?

PART II:

THE INVESTIGATION CONTINUES

- Through her MSSP, Jane engages a forensics team ("FT") to come in and confirm that the situation is contained, and to investigate and see if there's any way to get to a root cause and an accurate scope of what happened.
- FT installs a detection client on all PCs and monitors the network for 30 days.
- During that time OMG receives reports of phishing (and gets phished themselves by the attackers) but other than the quarantined Emotet variant, no other malicious software is found, and the AV solution seems to be quarantining everything.
- OMG already employs GPOs to enforce user context for all users (no exceptions), uses separate ADM accounts for administrators, blocks the ability to write to/execute from removable media and has a strong email filter and web proxy solution. The SIEM logs don't readily indicate any large traffic flows or other malicious traffic patterns.

How could this have happened?

How might they limit scope?

What more can they do to mitigate future attacks?

Tabletop Exercise 2 – Controls Scenario

Your public company, ABC Wealth Management, was informed by the SEC that a hacker by the name of "Tailgater" was bragging on the dark web about how he was able to make a tidy profit from the recent sale of your XYZ Wealth Management division.

To back this up, the hacker posted several documents he claimed were stolen from ABC prior to the sale (some of them even had document numbers in the footers.) Your CEO Joe Businessperson, and others working on the XYZ deal, are certain they did not share these documents with anyone other than the people directly involved with the sale.

PART I:

THE INVESTIGATION

- Joe's laptop shows no evidence of malware. Analysis of web traffic also did not show anything unusual, and as far as they could tell none of the secure file sharing site's technical cyber security controls failed.
- IT then asked around on Joe's floor, and the marketing director mentioned she did see someone in Joe's office and thought he was from IT. After getting a description of this individual, Facilities looked at security footage and saw an individual casually walking into the lobby elevators with a backpack that looked empty coming in, and full going out three hours later.

CONTEXT

- Joe has a habit of letting the 30-minute activity timeout lock his computer. IT staff found over 2GB of files saved locally in folders on his laptop, many of which were not filed to the document management system - and were also included in "Tailgater's" data dump on the dark web.

Who should be doing what (as part of incident response)?

What additional controls might have helped?

What is your communication strategy?

CONTROLS SCENARIO, PART II:

THE INVESTIGATION CONTINUES

-
  - Two days later, Jane Businessperson, who sits on the floor above Joe, reports that she can't find four paper folders she had checked out from the Records Department. These folders contained documents for a prominent private portfolio customer, a famous teen T.V. star whose trust ABC manages. They included a significant amount of PII, as well as information on electronic funds transfers that occur regularly from the trust to personal bank accounts.
  - No one can recall seeing anyone in Jane's office as she and her assistant were both out on vacation (and her assistant is still out for another week). Jane was certain the folders were on her desk when she left.
  - Later that afternoon, a story breaks that someone at the T.V. star's bank was tricked into wiring a large sum from a trust account to an overseas account. The bank stated on camera that the notice to change the account seemed to "come from ABC."

How do you manage this new development?

What evidence is there that these items were stolen?

What is ABC's overall liability?

Tabletop Exercise 3 – Nation State Scenario

Last month, Imaginary Law Firm LLP (ILF) received an official communication from the Czechoslovakian government alleging three of their clients have questionable connections to a group that attempted a drone-based assassination of a group of top government officials last year. The letter accuses the law firm of stirring political unrest and threatens retaliation. In a televised speech last week, the Czechoslovakian Prime Minister named the firm a "tool of terrorists" and publicly threatened retaliation.

Within days of the broadcast, ILF employees receive a suspicious email containing a "secure file" link that appears to be from one of their asylum-seeking clients. However, it's not actually from the client, it's a tailored phishing campaign aimed at the law firm, spoofing their client using an email address similar to the one the client actually uses.

PART I:

THE INVESTIGATION

- Shortly after the emails start coming in, the SIEM and EDR solutions send alerts and an investigation is initiated.
- Credential harvesting tools are discovered on the email server along with a cache of compressed video files that contain random confidential documents and emails not related to this specific case, some of which contain ILF letterhead.
- A hacker group sympathetic to the Czechoslovakian government releases "a set of ILF documents" on Twitter.

CONTEXT

- ILF uses two-factor authentication, application whitelisting and user context enforcement.
- Some exceptions are granted to "rainmaker" partners so that they can still install software when necessary in an emergency.

What technical issues should they immediately address?

What actions should management take?

How should ILF handle internal/external communications?

NATION STATE SCENARIO, PART II:

THE INVESTIGATION CONTINUES

- Two senior partners (rainmakers) were used to gain a foothold in the network.
- Leveraged MS Office macros and Admin session rights.
- Pivoted to virtual servers and stole the credentials of a system administrator to gain access to the email servers and other virtual machines.
- The cache of files is legitimate and goes back 20 years (stolen from mailboxes).
- Investigators discovered and stopped a live (incrementally growing) cache of illegal pornographic material, racist manifestos and other material common on Dark Web sites.
- Identified multiple SSL/TLS-encrypted connections on the laptops of two of the lawyers working the related asylum case. In both cases, these connections and data caches pre-date the current incident.

How has the scope of the incident expanded?

What additional damage control steps would you take?

How would you revisit the risk vs value of allowing executive exemptions to "restrictive" policies?