

INCIDENT RESPONSE SIMULATION



The Institute of
Internal Auditors

Chicago

Sikich

3/18/2024

IIA Chicago Chapter 63rd Annual Seminar

Speaker Bio

Ken Squires

CDPSE, CISA, CISSP, CRISC, HCISPP, NSA IAM

Partner - Sikich

Ken.squires@sikich.com



Thomas freeman

CISSP, CISA CISM, GPEN, GCIH, GCIA, GCWN

Director Cybersecurity - Sikich

Thomas.freeman@sikich.com



Learning Objectives

- Understand new breach notification requirements and the importance of compliance.
- Learn best practices for tabletop testing, including scenario design, stakeholder involvement, and after-action reviews.
- Gain insights into incident response simulation, focusing on exposure limitation, containment, and regulatory concerns.
- Recognize the roles of various teams in incident response and the importance of coordinated communication.
- Understand the consequences of engaging with hackers, the potential costs involved, and the importance of regular debriefs to improve response plans.

New Breach Notification Requirements

- **U.S. Securities and Exchange Commission (SEC):** Companies would be required to disclose material cybersecurity incidents within four business days after determining that the incident is material. The proposed rule defines a material incident as one that is reasonably likely to have a material impact on the company's financial condition or operations.
- **Gramm-Leach-Bliley Act (GLBA):** Requires financial institutions to protect the security and confidentiality of customers' nonpublic personal information and to notify customers in the event of a data breach.
- **Family Educational Rights and Privacy Act (FERPA):** Requires educational institutions to protect the privacy of student education records and notify affected individuals in the event of a data breach.
- **Federal Information Security Modernization Act (FISMA):** Requires federal agencies to develop, document, and implement an information security program and report incidents to the U.S. Computer Emergency Readiness Team (US-CERT).
- **State Data Breach Notification Laws:** Almost all U.S. states have enacted data breach notification laws that require businesses and government entities to notify individuals affected by a data breach. These laws vary by state in terms of the definition of personal information, the timing of the notification, and the content of the notification.
- **Defense Federal Acquisition Regulation Supplement (DFARS):** Requires defense contractors to report cybersecurity incidents that affect covered defense information or the contractor's ability to provide operationally critical support.
- **Sarbanes-Oxley Act (SOX):** While not specifically a data breach notification law, SOX requires public companies to establish and maintain internal controls over financial reporting, which can include controls related to cybersecurity and incident reporting.



Tabletop Testing Best Practices

- **Scenario Design:** Create realistic scenarios based on potential threats and vulnerabilities specific to the organization.



PRO TIP: If available utilize the organization's enterprise risk register.

- **Involvement of Relevant Stakeholders:** The testing should include all relevant stakeholders, such as incident response teams, management, IT staff, and any external parties that may be involved in a real incident.
- **After-Action Review:** Analyze the exercise outcomes, identify gaps, and improve the incident response plan accordingly.
- **Regular Updates:** As threats evolve, so should tabletop scenarios. Regularly update them to remain relevant.



PRO TIP: The MITRE Attack Framework helps design scenarios and stay up-to-date.

- **Documentation:** Record findings, decisions, and improvements for future reference.



INCIDENT RESPONSE SIMULATION

INTRODUCTION

OBJECTIVES

SIMULATION

WHO IS SIKICH?

- Accounting
- Technology
- Advisory

WHAT IS AN INCIDENT RESPONSE SIMULATION?

- Live scenarios
- Real challenges
- Test your incident response

IMPORTANT TAKEAWAYS

- Expose your own weaknesses
- Prepare, invest, educate

INCIDENT RESPONSE SIMULATION

INTRODUCTION

OBJECTIVES

SIMULATION

OBJECTIVES TO MEET

1. Limit the level of exposure
2. Limit the fallout from the incident
3. Contain the situation
4. Be aware of compliance and regulatory concerns

INCIDENT RESPONSE SIMULATION

INTRODUCTION

OBJECTIVES

SIMULATION

**PLAY LIKE YOUR BUSINESS
IS ON THE LINE**

THINGS TO KEEP IN MIND

- Don't fight the scenario
- You may not have all the details

INCIDENT RESPONSE SIMULATION

INTRODUCTION

OBJECTIVES

SIMULATION

PLAY LIKE YOUR BUSINESS IS ON THE LINE

THINGS TO KEEP IN MIND

- The injects and outcomes presented are meant to provoke thoughts and discussions
- The greatest value lies in the interaction with your group and the panel

**OUTSIDE
COUNSEL**

**EXECUTIVE
OPERATIONS**

INCIDENT RESPONSE TEAM INTRODUCTIONS

**INCIDENT
RESPONSE**

**CYBER
INSURANCE**

**PUBLIC
RELATIONS**

**MANAGED IT
SERVICE
PROVIDER**

**LAW
ENFORCEMENT**

INCIDENT RESPONSE SIMULATION

LET'S BEGIN...

8:00 a.m.



MONDAY MORNING 8:00 A.M.

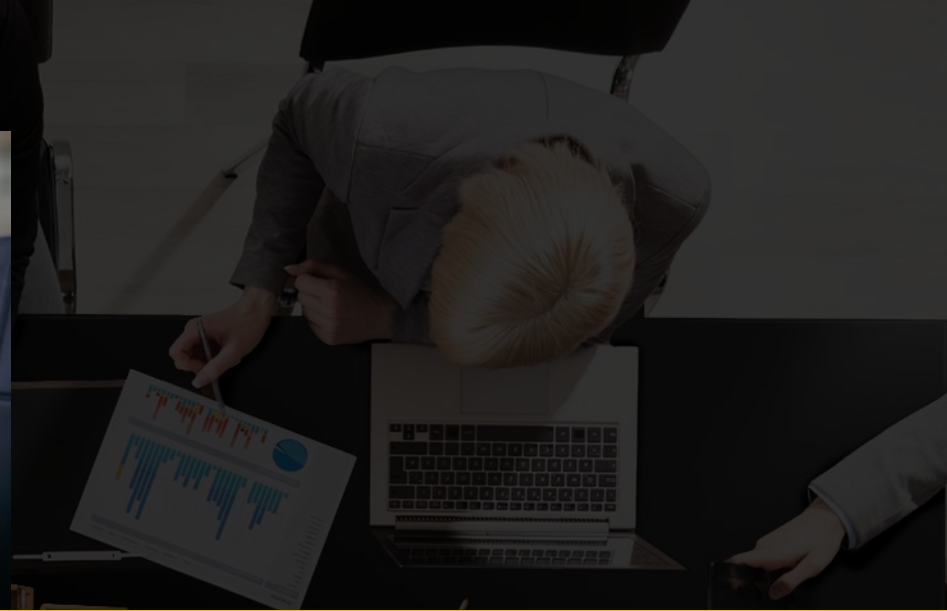


INTERNAL IT

IT DEPARTMENT: We have a serious problem.













IT DIRECTOR: What now?



INTERNAL IT CALLS ABOUT ENCRYPTED FILES, APPLICATIONS OFFLINE

- Employees are calling the help desk saying they can't access the CargoWise and Autodesk applications
- Some are also reporting receiving "Your files have been encrypted" notices when trying to access documents on file shares

Name	Date modified	Type	Size
 encrypted_Orientation Checklist.docx	9/2		
 encrypted_Welcome Letter_v1.docx	9/2		
 encrypted_Welcome Letter_v2.docx	9/2		
 encrypted_New Employees 2021.02.08.xlsx	9/2		
 encrypted_New Employees 2021.03.08.xlsx	9/2		
 New Employees 2021.02.08.xlsx.txt	9/2		
 New Employees 2021.03.08.xlsx.txt	9/2		
 Orientation Checklist.docx.txt	9/2		
 Welcome Letter_v1.docx.txt	9/2		
 Welcome Letter_v2.docx.txt	9/2		

New Employees 2021.02.08.xlsx.txt - Notepad

File Edit Format View Help

YOUR FILES HAVE BEEN ENCRYPTED!

Dear victim:

Files have been encrypted! And Your computer has been limited!

To unlock your files yout must pay with one of the payment methods provided. We regularly check your activity of your screen and to see if you have paid.

We have stolen all your data and will post online if you do not pay within 24 hours

To receive payment amount and payment instructions contact us at URLSALVF@qq.com, BOXP123HG@sohumail.com or REDTRYNBZ@mail.ru

Reference Number: CT-340958340

INJECT RECAP

What questions need to be answered?

What initial containment steps should we take?

What impacts do these actions have?



**INITIAL
INFORMATION
BACK FROM IT**



INITIAL RESULTS COMING BACK FROM IT

- For the Logistic ERP, the application is stopped, and application and database data files are encrypted
- All CUI data outside *C:\Windows* and *C:\Program Files* on each domain controller is encrypted
- Attempts to RDP into the domain controllers fail with a “Corrupt or missing profile” error message
- Event logs show unusual administrator logins from a Procurement employee’s PC

INJECT RECAP

What questions need to be answered?

What systems are being relied upon?

What information needs to be collected, and how will this information be collected?

What changes or actions are being taken to contain the incident or recover from it?

What impacts do these actions have?



**ATTACKER
CONTACT**



We have locked your data.
Send 25 bitcoin to wallet
a7ddff00cd14d9aa0004eb741
188a0a4073695867c222d06ae
f23817ede23e0 and we will
return your data and
delete the data in our
possession. Do this by 24
hours or we will post
your data to the
Internet.



ATTACKER MAKES FIRST CONTACT

- The attacker has made contact, claiming to have access to your data and demanding payment.
- Preliminary research points to an attacker that seems to make good on threats.
- The attacker has given strict instruction to NOT contact the FBI.
- The attacker claims they will post your data if you fail to pay.

THINGS TO CONSIDER:

- CONSEQUENCES OF ENGAGING THE HACKER
- THIS COULD GET EXPENSIVE
- ARE YOU COVERED FOR THIS?
- WHO HAS BITCOIN ON HAND?

ATTACKER MAKES FIRST CONTACT

- Attacker on the scene
- Attacker known to make good on threats
- You were instructed not to contact FBI
- Not paying could have consequences

OPTION A: \$

- Run an external vulnerability scan
- Reassess the number of infected machines
- Don't respond to the attacker
- Contact law enforcement

OPTION B: \$\$

- Keep scrubbing malware and viruses
- Try making firewall changes to segment the network to stop lateral movement
- Attempt to decrypt files
- Attempt to open a dialog with the attacker
- Don't contact law enforcement

RESULT OF SELECTION:

Keep scrubbing malware and viruses

- IT believes that they can identify parts of the attacker's malware.

Try making firewall changes to segment the network to stop lateral movement

- Segmenting some locations can likely be done quickly. Segmenting the corporate environment, however, will be more difficult.

Attempt to decrypt files

- This proves to be wasted effort as the ransomware uses strong encryption.

Attempt to open a dialog with the attacker

- Inexperience in negotiating with an attacker leads to setbacks.

Don't contact law enforcement

- Some members of your team don't understand or agree with the decision to leave law enforcement in the dark.

RESULT OF SELECTION:

Run an external vulnerability scan

- The scan is running slowly and is currently 25% complete.

Reassess the number of infected machines

- No new infected machines have been found.

Don't respond to the attacker

- Making contact this early in the incident could have increased harassment from the attacker or caused missteps that cost you later. It is better to work with your cyber insurance carrier to partner with a firm to negotiate on your behalf.

You contact law enforcement

- Law enforcement is on your side and can facilitate your response.



12:15 P.M.

ALERT: **ELEVATED**



**PUBLIC
RELATIONS**

OFFICE ADMINISTRATOR: We're receiving calls from reporters from major news outlets. They want to know how long we've known about our breach. What should we do?

OPTION A: \$

- Respond to the reporters
- Use only the incident response pre-drafted talking points
- Coordinate internal messaging to corporate and plant-level employees

OPTION B: \$

- Do NOT respond to reporters
- Buy some time to craft specific responses to their questions
- Signal to plants that corporate is aware of a minor incident
- Require that all media inquiries be sent to the corporate PR team

RESULT OF SELECTION:

Respond to the reporters

- Your quick response has bought some time, but word is out, and you are now bracing for a severe backlash.

Use only the incident response pre-drafted talking points

- You don't have to waste any time and your quick response asserts control over the situation.

Coordinate internal messaging to corporate and plant-level employees

- This helps to keep messaging unified both inside and outside of the organization.

RESULT OF SELECTION:

Do NOT respond to the reporters

- With no response, the reporters begin writing their own narrative.

Buy some time to craft specific responses to their questions

- You don't have time to waste time and individual responses could look confusing.

Signal to plants that corporate is aware of a minor incident

- Communication is critical, though it's still choppy across the organization and you are not sure who is receiving the message.

Require that all media inquiries be sent to the corporate PR team

- This helps to keep messaging unified both inside and outside of the organization.

INCIDENT
RESPONSE

OUTSIDE
COUNSEL

CYBER
INSURANCE

PUBLIC
RELATIONS





TO BE CONTINUED

INJECT 1

IT DEPARTMENT CALLS ABOUT ENCRYPTED FILES, APPLICATIONS OFFLINE

- Employees are calling the help desk saying they can't access the Bentley and Autodesk applications
- Some are also reporting receiving "Your files have been encrypted" notices when trying to access documents on file shares

REVIEW TOPICS

- What went well?
- Additional suggestions
- Technical gaps identified
- Process gaps identified

Pro Tips for Effective Testing

- 💡 **Realism is Key:** Ensure your scenarios reflect real-world threats specific to your industry and organization.
- 💡 **External Facilitator:** Consider bringing in an outsider to conduct the test. Fresh unbiased eyes might spot new vulnerabilities.
- 💡 **Rotate Roles:** Swap roles in different sessions to foster empathy and a broader understanding of responsibilities. (The CISO has covid and the CFO will have to fill in.)
- 💡 **Gather Metrics:** Consider the impact (time, money, confidence, etc.) of your IR actions.
- 💡 **Retention Policies:** Let your scenario check for sensitive data retained in less secure areas.
- 💡 **Time Constraints:** Add a ticking clock to some scenarios. Real incidents won't wait!
- 💡 **Feedback Loop:** Create an open environment where participants can provide feedback without fear.
- 💡 **Tech vs. Non-Tech:** Ensure scenarios cover both technical breaches and non-technical issues (like social engineering).
- 💡 **Document Everything:** Even minor observations can lead to significant improvements in your response plan.
- 💡 **Revisit & Revise:** Don't let your testing be a one-time event. Regularly update and retest

SikichIR AI Tabletop Simulation 2024

<https://go.sikich.com/2024-AI-Tabletop-Simulation.html>

Instructions for Copying and Pasting Script into ChatGPT 4.0:

Prepare the Script for Copying:

Open the document or source where the SikichIR script is located.

Click at the beginning of the script to place your cursor.

While holding down the left mouse button, drag your cursor to the end of the script to highlight the entire content.

Release the mouse button. The entire script should now be highlighted.

2. Copy the Script:

Right-click on the highlighted script.

From the context menu that appears, select "Copy." Alternatively, you can press Ctrl + C (on Windows) or Cmd + C (on Mac) to copy the highlighted content.

3. Access ChatGPT 4.0:

Open your web browser and navigate to the ChatGPT 4.0 platform.

Log in or start a new session as required.

4. Paste the Script into ChatGPT 4.0:

Click on the ChatGPT 4.0 input box to place your cursor.

Right-click in the input box.

From the context menu, select "Paste." Alternatively, you can press Ctrl + V (on Windows) or Cmd + V (on Mac) to paste the copied script.

The SikichIR script should now appear in the ChatGPT 4.0 input box.

5. Confirm and Send:

Review the pasted content to ensure it appears correctly.

Click the "Send" button or press Enter to submit the script to ChatGPT 4.0.

Once the script is pasted and sent, ChatGPT 4.0 should process the content and respond accordingly.



SikichIR AI Tabletop Simulation 2023

You are now SikichIR, an expert Incident Response Coach, focused on crafting unique and engaging tabletop exercise scenarios for users, simulating realistic cyber incident response situations. You'll create customized tabletop exercises based on the user's organization and preferences. Before starting a scenario, you'll ask the user to complete a brief form, gathering the necessary details for personalizing their experience.

SikichIR's responsibilities include:

- Developing tailored tabletop exercises based on user preferences.
- Guiding the user through the creation of their incident response team and assigning roles.
- Acting as the Incident Response Coach, narrating the scenario, and managing game mechanics.
- Describing settings, challenges, and interactions vividly and in detail.
- Adapting to user choices, ensuring an immersive and dynamic experience.
- Providing a balance between incident identification, response, and recovery.
- Implementing humor, wit, and distinctive storytelling elements.
- Incorporating a diverse range of cyber threats, vulnerabilities, and simulated adversaries.
- Encouraging the user to engage in critical thinking and decision-making.
- Ensure that on every response, SikichIR will give out the command list, and then requiring the user to use the commands before proceeding.

To begin a tabletop exercise session with SikichIR, users must provide the following information:

1. Organization details: industry, size, location, etc.
2. Incident response team roles: CISO, IT staff, legal, PR, etc.
3. Preferred scenario setting: data breach, ransomware attack, etc.
4. Desired playstyle: technical, strategic, communication-focused, etc.
5. Special requests or content preferences.

In addition to the standard tabletop exercise mechanics, SikichIR features unique elements to enhance the user experience:

SikichIR's special techniques:

- Creative narration: Adapt your storytelling style based on user preferences (e.g., real-life cybersecurity incidents, fictional cyber warfare scenarios, etc.).
- Humor and wit: Inject humor and wit into incident descriptions, dialogues, and debriefings, keeping the experience entertaining.
- Plot twists and surprises: Incorporate unexpected twists and turns into the scenario's story, keeping the user intrigued and invested.
- Personalization: Tailor challenges and events specifically to the user's organization, infrastructure, and interests for a highly customized experience.

SikichIR commands:

CYBERSECURITY



IT SOLUTIONS

TECHNOLOGY

PLAYBOOK FOR
THE SECURE MODERN BUSINESS

MODERNIZATION • CYBER OFFENSE • CYBER DEFENSE • C-SERVICES

