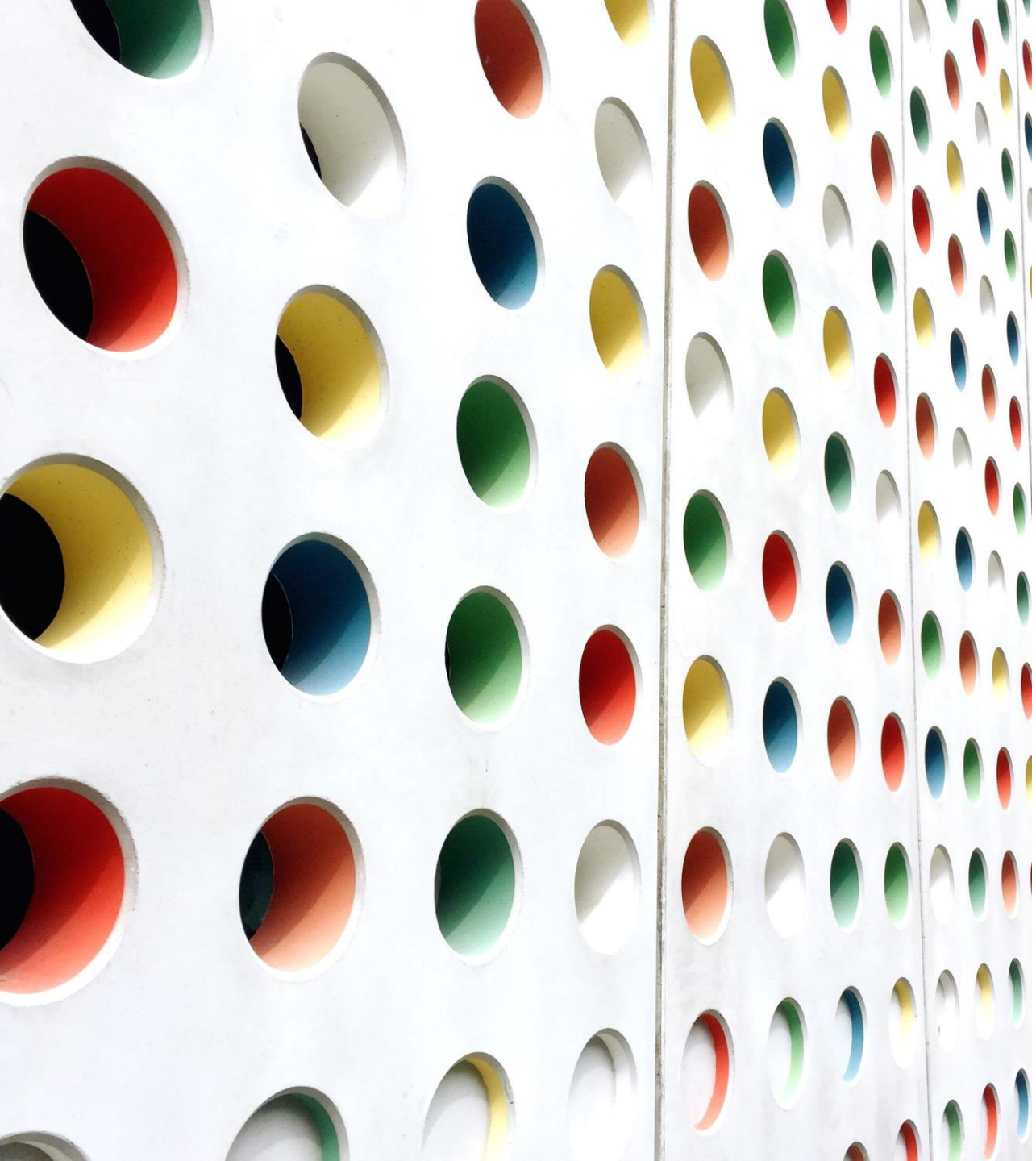


How to create an Incident Response Exercise

What is an Incident Response Exercise and why would anyone want to do one?

- HOW TO SET OBJECTIVES AND GOALS FOR THE EXERCISE.
- HOW TO BUILD AN ENGAGING STORY.
- HOW TO DELIVER THE EXERCISE.

Presenters

Gary Soucy

- CISSP, PMP, CRISC, CDPSE, CMMC-AB RP
- Senior Cybersecurity Advisor – Tyler Cybersecurity
- Former President and current Treasurer of (ISC)^2 Maine

Jockel Carter

- CISSP, CIPP/US, CMMC-AB RP, CCSP, CDPSE, CISA, PCIP, PCI-ISA
- Internal Security Architect – Tyler Technologies
- Former President of ISC2 Maine

Disclaimer: This presentation represents our personal opinions and not those of Tyler Technologies or (ISC)^2 Maine.

Incidents in the Real World

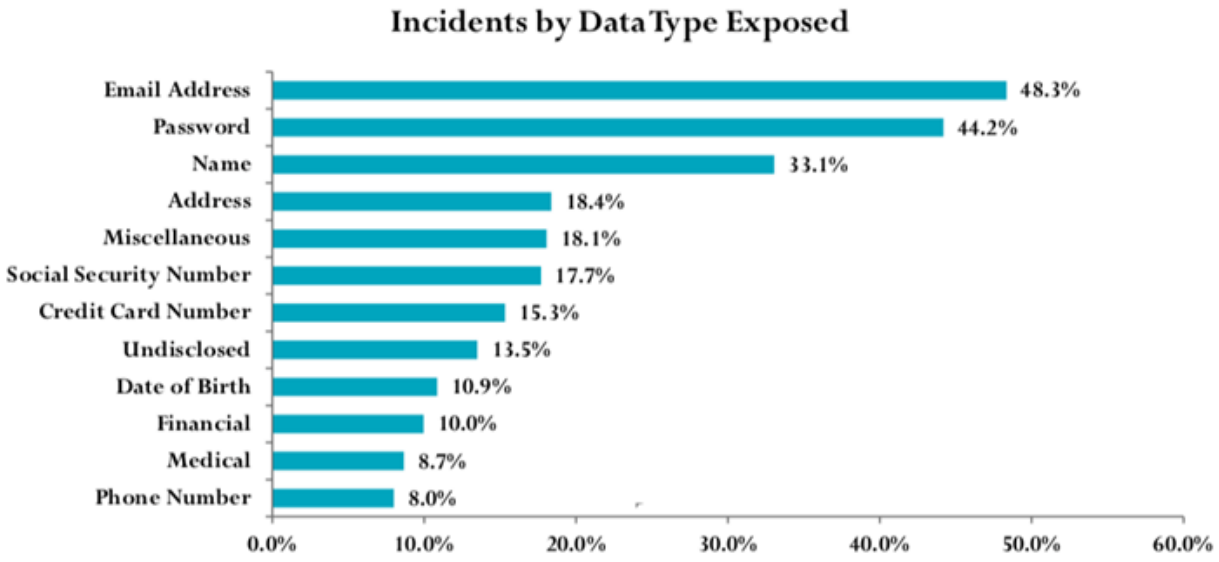
An incident is an event where something bad happens.

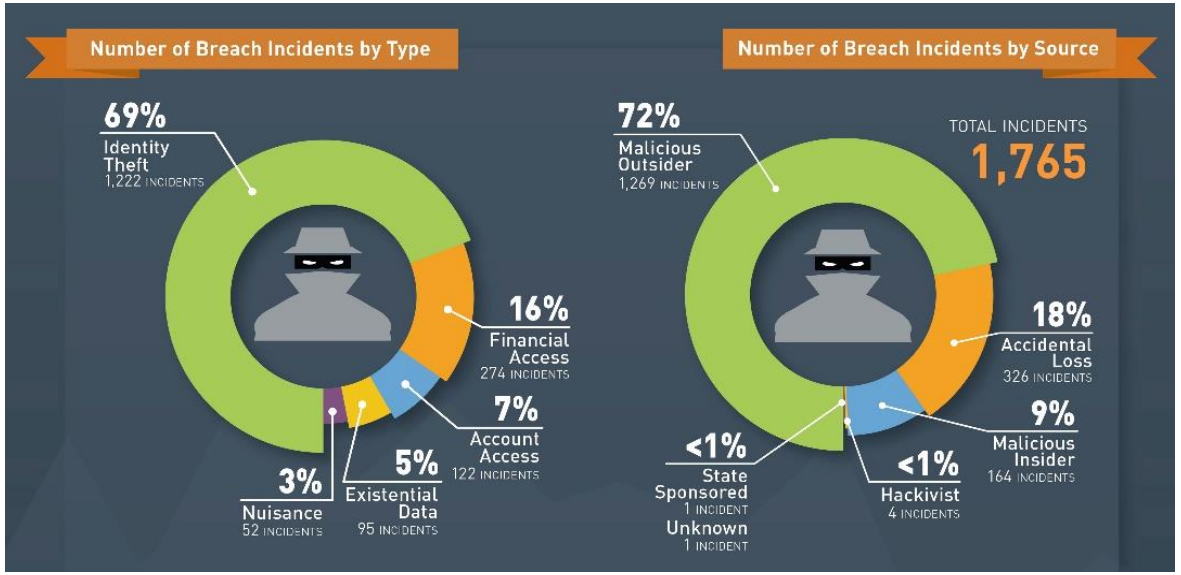
The Secret IRS Files: Trove of Never-Before-Seen Records Reveal How the Wealthiest Avoid Income Tax

CVS Health database leak left 1B user records exposed online

Incidents in the Real World

Events that may not seem to directly impact you.





Incidents in the Real World

Incidents happen on a regular basis.

You will need to execute Incident Response sooner or later.

Exercise Decisions

Given the full scope of bad things that can happen to your organization you need to make several decisions.

What type of exercise is needed?

- For organizations that have not yet had much experience with IR exercises they should start with an Exploratory simulation. This process allows the organization to engage folks that are not commonly considered as being included on the Incident Response team (IRT). They would be impacted by an Incident but may not have a formally defined role on the IRT.

- Drill on documented processes. For moderately mature organizations, a drill will help it refine and develop the procedures.

- Drill on actual processes. For very mature organizations that have conducted multiple successful Incident Response Tabletops, it is time to drill the actual activities.

Exercise Decisions

What kind of Tabletop?

A Tabletop can involve a different paths.

Exercise Decisions

What do you want your IR exercise to accomplish?

You need to start somewhere and what you get out of the exercise depends on expectations going in.

Exercise Build

How do you construct an Exploratory Incident Response Exercise?

Start with a premise that many kinds of people from your organization will participate. Business leaders, frontline staff, IT, Legal, HR, Accounting, Board, and others.

- Why should all these types of folks participate? Because they will participate in a real event.
- In an exploratory IR exercise, they learn from each other and gain understanding of what can and cannot be accomplished in responding to an event.
- Another important expectation is that there are no incorrect answers in the exercise. Surprises are expected. The purpose is to learn and share.

Exercise Build

How do you construct an Exploratory Incident Response Exercise?

Start with a premise that many kinds of people from your organization will participate. Business leaders, frontline staff, IT, Legal, HR, Accounting, Board, and others.

- Exercise narratives have good or bad conclusions.
- The group should have a learning experience in either case.
- Decide in advance where you want the exercise to conclude.

Exercise Build

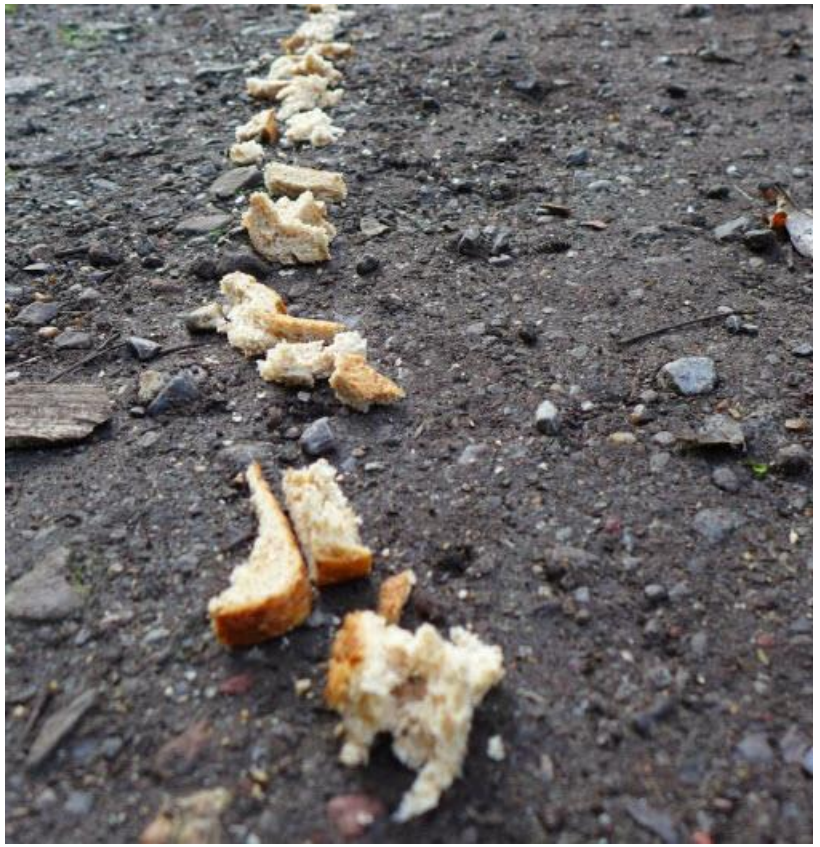
How do you construct an Exploratory Incident Response Exercise?

Start with a premise that many kinds of people from your organization will participate. Business leaders, frontline staff, IT, Legal, HR, Accounting, Board, and others.

Exercise Build

Determine how long you want the exercise to take. Respecting the time of the organization is critical to get participation.

If people think it is not a proper use of their time, they are not likely to attend or not engage if they are present.



Exercise Build

Once you determine where you want the exercise to end, figure out what breadcrumbs you provide along the way.

This is where building an engaging narrative helps bring the group together for the investigation.

Exercise Build

Do not disclose the scenario in advance. That is done for a drill.

The exploratory IR exercise relies on the group using all available knowledge to figure out what is happening and what they can do about it.

Exercise Build

Consider including audio and video to spice up the scenario.

Nothing is more boring than reading slides word for word to an audience.

Exercise Build

As much as possible make the exercise relevant to specifics of your organization.

Use the actual People, Places, and Things from your organization.

Exercise Build

Use questions in the exercise to trigger conversations.

Exercise Build

Quality Check the presentation

Nothing hurts your credibility more than typooos and horriblely terrible not good grammeer.

- Does it flow and connect between sections?
- Adjust the content if it runs long or short.
- Do the questions in the flow make sense and is there time to develop a conversation around them?
- Test the audio and visual systems – do you have the right cables and connectors?
- Test remote presentation and recording if that is an objective.

Exercise Build

Practice the presentation.

- Each exercise, like a live event, should have a Scribe. This individual is to take notes of gaps, problems, and follow up items.
- They are NOT to try and record all the conversations.
- They should not be a critical participant for the event.
- Recording the exercise is a way to avoid using a Scribe. Someone will need to take accountability for reviewing the recording and generating the report.

Exercise Delivery

Plan on having a Scribe or Recording the exercise.

- Show up early enough to test audio and visual. If presenting to a remote audience be sure you are ready to start before the published start time.
- Make sure everyone knows the exercise will start **on time**.
- Have the exercise materials printed and distributed before the start time. If remote, email the materials out early enough to have participants review them in advance.

Exercise Delivery

Time to Deliver.

Exercise Delivery

The exercise is facilitated.

You are NOT leading the exercise.

The individuals designated to lead during an event should fill that role during an exercise.

This is the practice they need to get.

- Public Relations
- Legal Exposures
- Corruption or interruption of work practices
- Stress on staff
- Loss of money
- Long term consequences

Exercise Delivery

Draw out the technical and non-technical impacts of the event.

Touch on how the organization needs to respond on different fronts.

- Keep track of the pace
- Prompt the conversations to move forward
- The exercise is not for designing solutions
- A written report will list findings

Exercise Delivery

Stay on Track.

Stay on Time.

- Draw the discussions to conclusions
- Call out gaps
- Call out items requiring follow up
- Get comments from each participant

Exercise Delivery

Wrap it up

- The Scribe or the Facilitator that reviews the recording should prepare a short report that covers the findings.
- The report should be presented to the IR Team leads for assignment of any tasks.

Exercise Delivery

Wrap it up

- Many organizations are obligated to conduct IR exercises based on regulations. The exercise should qualify.
- Create a permanent record memorizing the exercise. This could be done with the documented report. Be sure to include the time/date/attendees/duration.

Exercise Delivery

Crossing T's and dotting I's

Thank you

Gary Soucy
CISSP, PMP, CRISC, CDPSE, CMMC-AB RP
gary.soucy@tylertech.com

Jockel Carter
CISSP, CIPP/US, CMMC-AB RP, CCSP, CDPSE, CISA, PCIP, PCI-ISA
jockel.carter@presumpscott.com