The CISO Is Dead

Now What?

December 5, 2024

Own

Introduction

Own

Introduction

- ilan Finkelstein –
    - Principal Security Architect – Security Development Team
    - ilan.Finkelstein@owndata.com
    - MSc in Cyber Security, NYU
    - BSc in Computer Science, John Jay
    - 4x AWS Certified, Member of ISC2

Introduction

- Pieter Vaniperen
  - Chief Information Security Officer
  - pieter.vaniperen@owndata.com
  - Former Deputy CISO - Clear, Fox, Disney
  - MSc in Cyber Security
  - 25+ Cyber Certifications

Overview

Overview

- Introduction
- Quick Review of Terminology
- Developing Real World Possibilities
- Introducing Randomness
- Conceptualizing Black Swan Events
- Gaining Management Buy In
- Including Others
- Conclusion

Terminology

Terminology (1)

Disaster Recovery (DR) –

An organization's ability to restore access and functionality to IT infrastructure after a disaster event, whether natural or caused by human action (or error). (GCP)

Terminology (2)

Incident Response (IR) –

Incident response is the actions that an organization takes when it believes IT systems or data may have been breached. For example, security professionals will act if they see evidence of an unauthorized user, malware, or failure of security measures. (MS)

Terminology (3)

Business Continuity Planning (BCP)-

Documentation of a predetermined set of instructions or procedures that describe how an organization’s mission / business processes will be sustained during and after a significant disruption. (NIST)

Terminology (4)

Black Swan Event –

Refer to events that defy expectations, carry extreme consequences, and are only understood in hindsight. (Forbes)

Developing Real World Possibilities

Own

Developing Exercises

Quality simulations rely on multiple factors:

- Clear purpose
- Well defined
- Authentic
- Interesting
- Exciting
- Unpredictable
- Inclusive
- Automated

Developing Exercises (2)

Clear Purpose -

Successful exercises begin with a straightforward and simple explanation of the goals.

Developing Exercises (3)

Well Defined –

Planning and explanation of what exactly is fair game, what is out of bounds goes a long way.

Developing Exercises (4)

Authentic–

Exercises need to be built on real possibilities and true potentialities for the organization.

Developing Exercises (5)

Interesting–

Excercises need to capture the groups attention and provide enough challenge.

Developing Exercises (6)

Unpredictable –

Exercises need to have enough randomness of events and outcomes that keep participants interested and "on their toes."

Developing Exercises (7)

Inclusive –

Create an exercise that removes the “typical cast of characters”, i.e. those usually involved in initial DR, IR or BCP activities.

Developing Exercises (8)

Automated –

Utilize Scripting and Automations to develop scenarios that unfold without game organizer interaction.

Introducing Randomness

Introducing Randomness

Randomness refers to the quality of lacking a definite plan. To provide this randomness to an exercise serves two purposes:

- Maintaining interest
- Providing Authenticity

Introducing Randomness (2)

Maintaining interest in not typical work activities can sometimes be hard. Limiting distractions helps but developing engaging and interesting circumstances that impact the overall experience of an exercise can keep participants involved and unsure of what the end state will be, much like real incidents.

Black Swan Events

Black Swan Events

Figuring out the one in a million possibilities can be difficult.
Creativity and understanding of the environment help.

Gaining Management Buy-In

Gaining Management Buy-In

Convincing your leadership that half of the Ops team, ¾ of Security and resources from legal, finance and Product need to all be in the same room for the next 8 hours and not at their desks can be a difficult ask.

Gaining Management Buy-In (2)

To make this happen, utilizing some understanding of the corporate environment, along with common statistics about the prevalence and importance of preparedness can be your friend.

Gaining Management Buy-In (3)

BCP Statistics:

- Continuity breaks cost between $137 to $16k per minute
- 9/10 Businesses experience one or more outages per quarter

Gaining Management Buy-In (4)

DR Statistics:

- Corporations lose 40% of employee productivity during outages
- 30% of organizations permanently lose data
- More than 2/3 of outages cost companies over 100k in revenue

Gaining Management Buy-In (5)

IR Statistics:

- Ransomware gangs collected $1.1 Billion in 2023
- 72.7% of organizations worldwide experienced ransomware attacks in 2023
- Cyberattacks exposed the health records of 1 in 4 people in the first 9 months of 2023

Including Others

Including Others

Once you have achieved management buy in, inviting other teams, peripheral to the actual technology teams enhances preparation and realism.

Including Others (2)

Teams to consider including:

- Legal
- Finance
- C-Suite
- Physical Security
- Marketing / PR

Conclusion

Own

Conclusion

Developing interesting, seemingly random exercises requires time, attention to detail, management buy in and a level of authenticity while being anything but run of the mill.

Conclusion（2)

Developing these exercises, while including members of departments peripheral to a technical outage enhances overall team unity, company cohesion and develops some level predictability for real world occurrences.

Conclusion (3)

Making these exercises fun while still interesting is time consuming and resource intensive. Ensuring organizational support, with the help of an executive sponsor along with clarity about what the exercise entails can ensure success.

Thank You

Own

Team Dark

Name Namerson

Position

Email@email.com

+000 000000000

Name Namerson

Position

Email@email.com

+000 000000000

Name Namerson

Position

Email@email.com

+000 000000000

Name Namerson

Position

Email@email.com

+000 000000000

Introduction

- Pieter VanIPeren
  - Principal Security Architect – Security Development Team