An IR Guide to Communicating with Execs

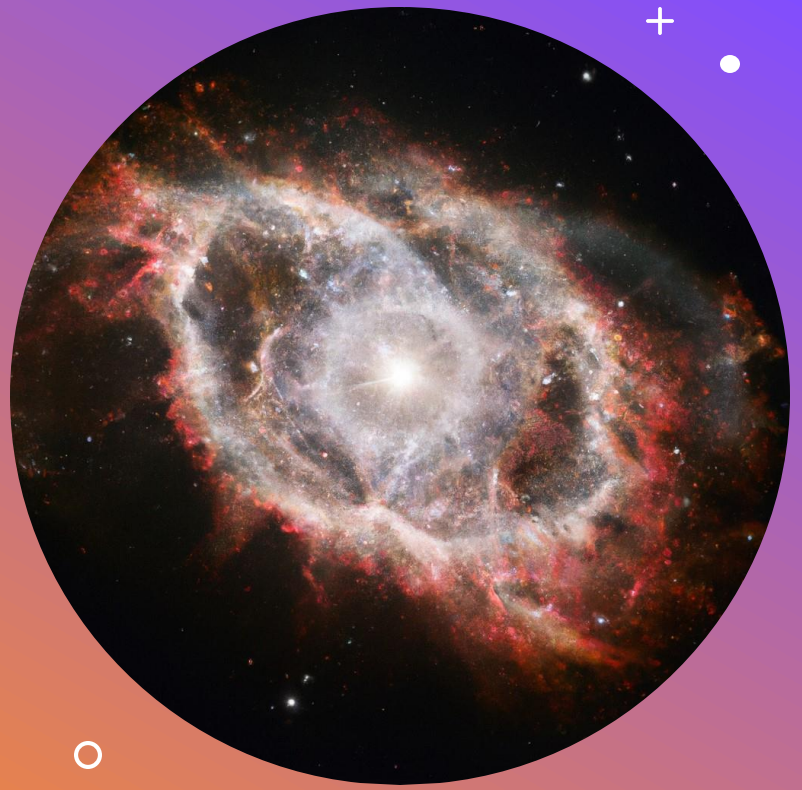
TEAM

Danielle Jamieson
Head of Cyber Wargaming

Anthony Kosednar
Cybersecurity Executive

Nate Thornton
Cybersecurity Operations Manager

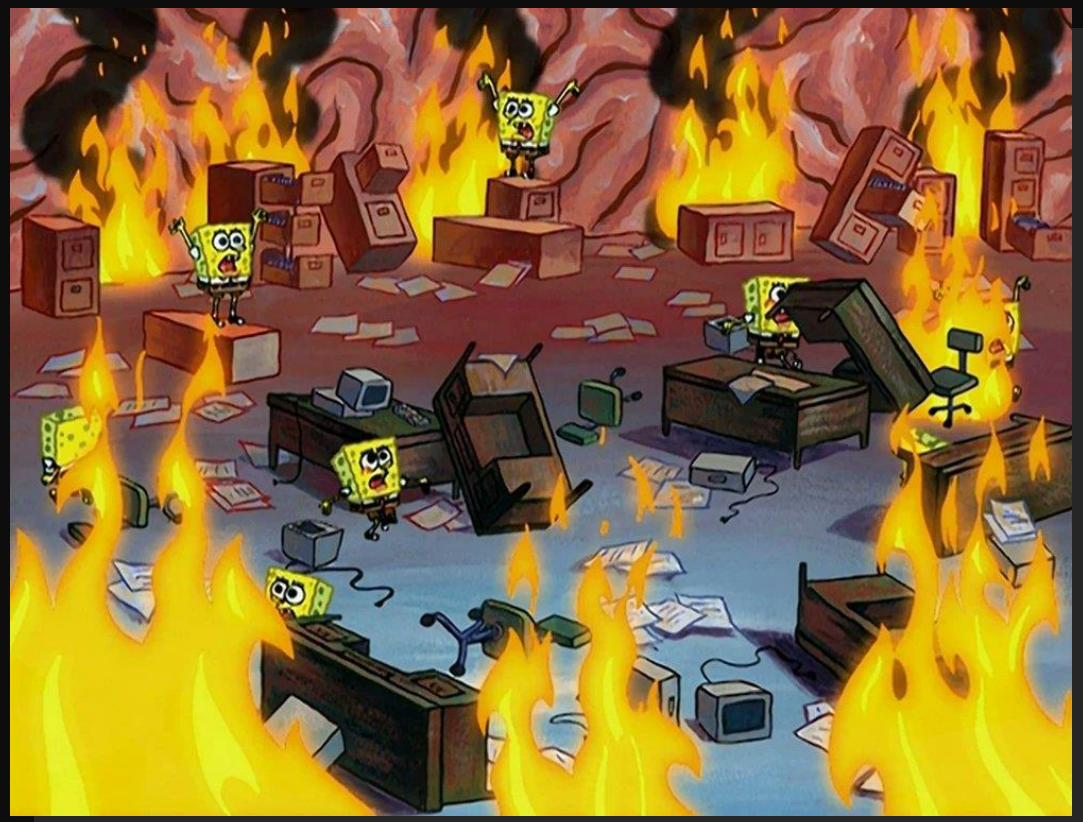
DON'T PANIC!: AN IR GUIDE TO COMMUNICATING WITH EXECS



AGENDA

- The Report at the End of the Universe
- Life, the Bad Examples, and How to Fix Everything
- The Ultimate IR Guide, Incomplete and Very Abridged
- So Long, and Thanks for All the Questions

The IR Team:



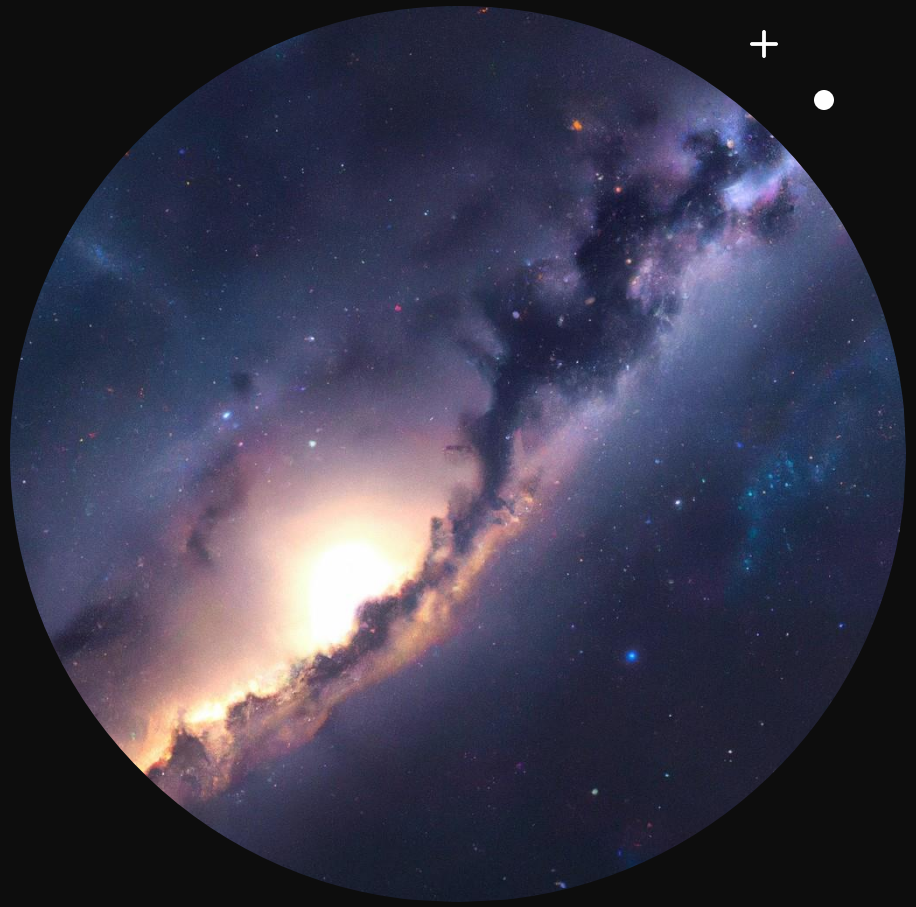
Management:

THE REPORT AT THE END OF THE UNIVERSE

What are we Actually Talking About?

Internal communications to executives and others outside of the security team during cybersecurity incidents

- How do you explain what's going on without unnecessarily freaking people out?
- … or maybe freaking them out the appropriate amount
- Our experience is in cyber, but this could theoretically apply to any type of incident communications



Writing Effective Reports

Remember your audience

- What level of expertise do they have?
- What do they care about?
  - Customer impact
  - Financial impact
  - Reputational impact

Get rid of unnecessary detail

- Keep it short
- Avoid jargon

Stick to the facts as you know them

- Don’t speculate
- Don’t bring feelings into it
- Use qualifiers where you're not sure: "at this time", "likely", "probable", etc.

Clear, concise writing is a skill

- Pull in someone who isn’t an expert, but is a great writer
- Consider making a designated role for reporting during critical incident response

Anticipate questions

- Answer questions before they’re asked

Everyone Needs an Editor

- Don’t take feedback personally

Structuring a Report

What happened?

- Very high-level. No details.

What is the impact to the business?

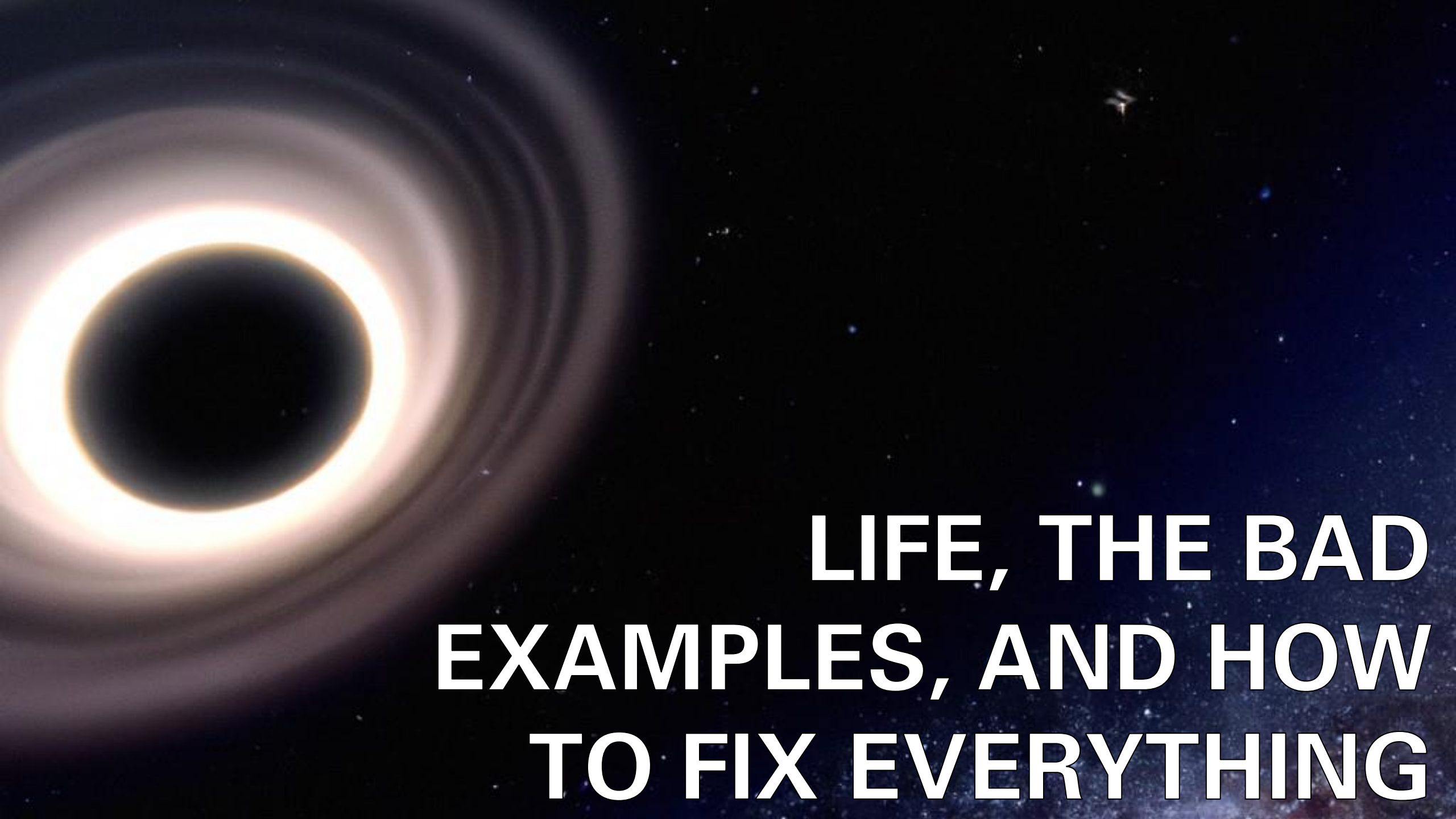
- Users impacted, data exposed, financial loss, etc.

What are we doing about it?

- Summarize incident response (IR) activities

How are we making sure this doesn't happen again?

- Report on this once things start to calm down



LIFE, THE BAD EXAMPLES, AND HOW TO FIX EVERYTHING

Example 1 | Too Technical

Situation: You are an incident responder at InfiniteProbability Technologies, Inc. The org was hit with a ransomware attack. The threat actor has encrypted systems and exfiltrated data.

Not Great:

> An APT utilized OSINT to pretext the TS hotline at InfiniteProbability. This resulted in domain admin, which allowed the APT to set up a C2 server and encrypt assets on the network using a 256-bit key and ChaCha20-Poly1305. Scattered Spider also exfiltrated PCI, NPII, and PII information while inhibiting system recovery (MITRE ATT&CK T1490). IR teams are eradicating the trojanized malware and obtaining forensic evidence for reverse-engineering.

Example 1 | Too Technical

Situation: You are an incident responder at InfiniteProbability Technologies, Inc. The org was hit with a ransomware attack. The threat actor has encrypted systems and exfiltrated data.

Not Great:

> An APT utilized OSINT to pretext the TS hotline at InfiniteProbability. This resulted in domain admin, which allowed the APT to set up a C2 server and encrypt assets on the network using a 256-bit key and ChaCha20-Poly1305. Scattered Spider also exfiltrated PCI, NPII, and PII information while inhibiting system recovery (MITRE ATT&CK T1490). IR teams are eradicating the trojanized malware and obtaining forensic evidence for reverse-engineering.

Much Better:

> A threat actor, Scattered Spider, utilized publicly available information to trick the technical support hotline. This allowed them to gain admin access and lock up devices on the network. The threat actor also exfiltrated sensitive information from 20,000 customers and 300 employees. The threat actor is preventing recovery of critical systems by destroying backups. The Incident Response team is working to collect evidence and remove the threat.

Example 2 | Too Scary

Situation: You are an incident responder at InfiniteProbability Technologies, Inc. and a new zero-day vulnerability in a popular application from Vogon technologies has been announced.

Not Great:

> A new highly critical zero-day vulnerability in Vogon technologies software has likely already been exploited on every internet-facing server in existence!!! One of our servers was compromised. This could result in all of our client-facing services being taken down, complete compromise of our entire network, and also will likely cause our stock prices to drop precipitously. I can already see protesters gathering outside the building!

Example 2 | Too Scary

Situation: You are an incident responder at InfiniteProbability Technologies, Inc. and a new zero-day vulnerability in a popular application from Vogon technologies has been announced.

Not Great:

> A new highly critical zero-day vulnerability in Vogon technologies software has likely already been exploited on every internet-facing server in existence!!! One of our servers was compromised. This could result in all of our client-facing services being taken down, complete compromise of our entire network, and also will likely cause our stock prices to drop precipitously. I can already see protesters gathering outside the building!

Much Better:

> A new zero-day vulnerability in Vogon technologies has been announced. This vulnerability is already being exploited in the wild. Two InfiniteProbability devices are impacted by this vulnerability and one is showing signs of compromise. The Incident Response team immediately took this device offline and there is no sign of further compromise in the network. Teams are currently starting forensic investigation of the compromised device.

Example 3 | No Action

Situation: You are an incident responder at InfiniteProbability Technologies, Inc. and a new zero-day vulnerability in the Somebody Else's Problem Field has been announced.

Not Great:

> A new vulnerability in the Somebody Else's Problem (SEP) Field has been discovered. InfiniteProbability does not use this product, but some of the firm's third-party vendors do. Hopefully they patch it soon, or else a lot of our customer's sensitive data could be exposed.

Example 3 | No Action

Situation: You are an incident responder at InfiniteProbability Technologies, Inc. and a new zero-day vulnerability in the Somebody Else's Problem Field has been announced.

Not Great:

> A new vulnerability in the Somebody Else's Problem (SEP) Field has been discovered. InfiniteProbability does not use this product, but some of the firm's third-party vendors do. Hopefully they patch it soon, or else a lot of our customer's sensitive data could be exposed.

Much Better:

> A new vulnerability in the Somebody Else's Problem (SEP) Field has been discovered. InfiniteProbability does not use this product, but the firm's third-party vendors do utilize SEP. The Incident Response team has engaged Vendor Management and requested that all critical vendors provide a detailed explanation of any impact that this vulnerability may have to InfiniteProbability data. At this time, there is no known impact to any company data or business processes.

Example 4 | Downplaying

Situation: You are an incident responder at InfiniteProbability Technologies, Inc. and it has been discovered that the new Kill-O-Zap blasters have been misfiring due to a configuration error.

Not Great:

> “It has come to the team’s attention that the default configuration of the new line of Kill-O-Zap blasters may result in misfires, though none have been reported at this time. No one uses the default configuration anyways, so we should be fine. Investigations did not discover any malicious threat. The misconfiguration has been corrected and overly permissive access to the configuration system was revoked.”

Example 4 | Downplaying

Situation: You are an incident responder at InfiniteProbability Technologies, Inc. and it has been discovered that the new Kill-O-Zap blasters have been misfiring due to a configuration error.

Not Great:

> It has come to the team's attention that the default configuration of the new line of Kill-O-Zap blasters may result in misfires, though none have been reported at this time. No one uses the default configuration anyways, so we should be fine. Investigations did not discover any malicious threat. The misconfiguration has been corrected and overly permissive access to the configuration system was revoked.

Much Better:

> It has come to the team's attention that the default configuration of the Kill-O-Zap blasters may result in misfires that could harm users or others. The configuration change was committed by a disgruntled ex-employee who maintained access to the system after termination. The misconfiguration has been corrected, the ex-employee's access has been revoked, and the team is currently investigating any other systems that the employee may have accessed post-termination.

THE ULTIMATE IR GUIDE

Incomplete and Very Abridged

Summary

Writing Tips

- Remember your audience
- Get rid of unnecessary detail
- Stick to the facts
- Clear, concise writing is a skill
- Anticipate questions
- Everyone needs an editor

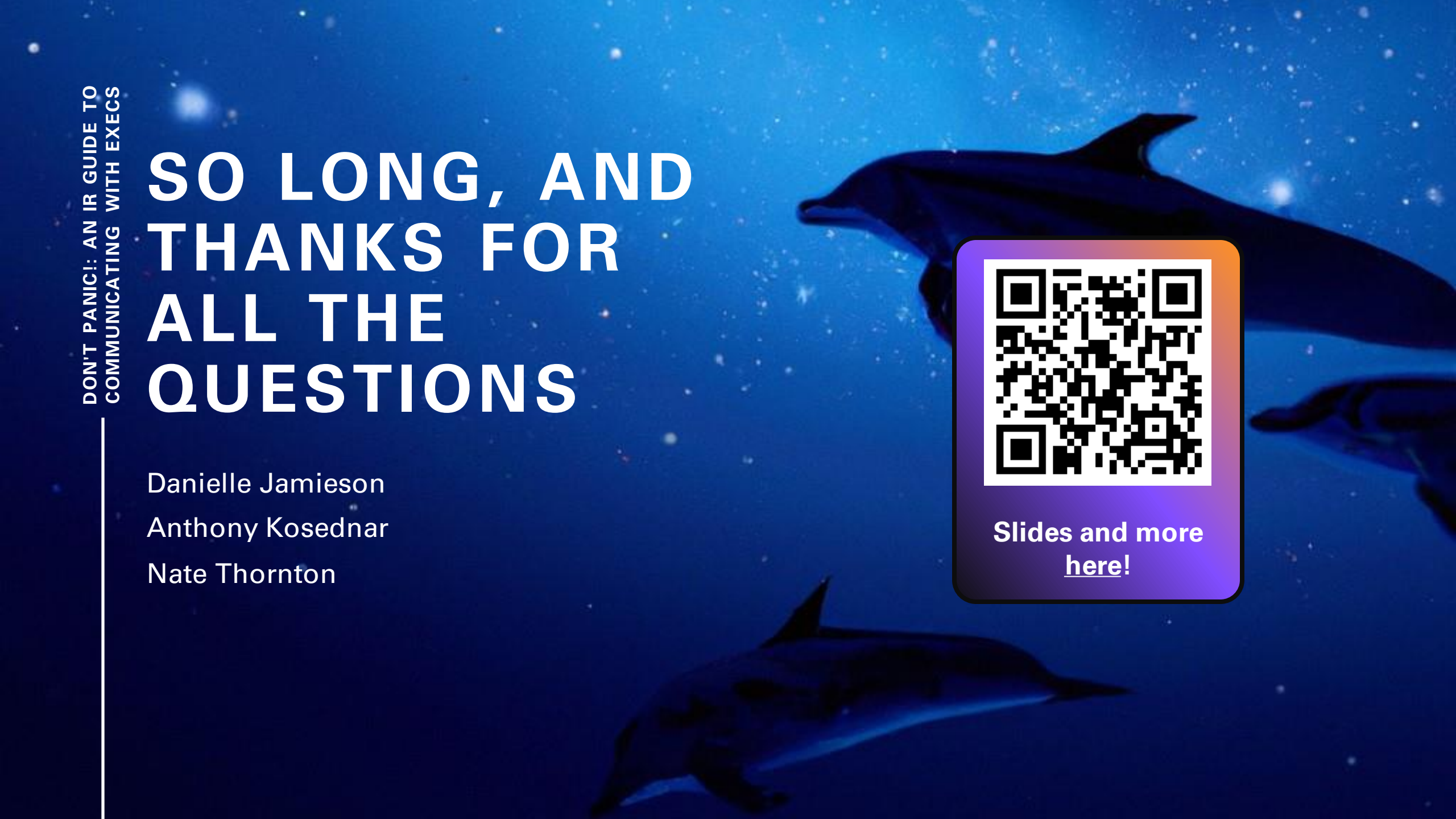
Report Structure

- What happened?
- What is the impact to the business?
- What are we doing about it?
- How are we making sure this doesn’t happen again?

DON'T PANIC!: AN IR GUIDE TO COMMUNICATING WITH EXECS

SO LONG, AND THANKS FOR ALL THE QUESTIONS

Danielle Jamieson
Anthony Kosednar
Nate Thornton



Slides and more here!