AON

Top 10 Things to Do (or Not Do) in the First 48 Hours

John Ansbach, Managing Director

Stroz Friedberg, an Aon company

1

AON

Top 10

- Act fast
- Don’t panic
- Get help
- Don’t blame
- Work together
- Don’t succumb to pressure
- Mind your regulatory obligations
- Don’t go cheap
- Set up secure communications channels
- Don’t Reach out to a threat actor on your own

2

AON

Do Act Fast

1

- Acting immediately when a breach is discovered (or even suspected) can dramatically mitigate impact, especially blast radius
- Culturally, you can give the greenlight to you technical teams to reach out for DFIR help even when they aren't sure there is an incident
  - Err on the side of caution
- Same goes internally
  - Yes, the CEO is on vacation with her family…so what. Ring the bell.

AON

Don't Panic

2

- Cybersecurity incidents can be highly emotional events
- Calm steady leadership will win the day
- Especially true where technology and information security team are stressed and sleep-deprived
- Be deliberate, set the tone, "we will get through this"

AON

Do Get Help

3

- You cannot do this alone
- Whether it's ransomware, third-party partner driven attack, or even a large scale BEC, digital forensics firms, as well as law firms, have experts who can help
- Get your forensics firm on the phone
- Get your outside counsel on the phone
  - Really important this happen right away
  - Attorney – client privilege, to the extent it can be secured – can only happen when lawyers are on the phone, on the email, etc.
- Get your insurance folks on the phone
- Get restoration and recovery teams on the phone (or in the building)

AON

Don't Blame

4

- Avoid the temptation to "hold someone accountable" *during* an IR
- There will come a time after the business has recovered to talk about why this happened, how it could have been avoided, and whether there were failures that merit personnel action
  - During an IR is *not* that time
- You need technology and information security leaders singularly focused on supporting investigation, containment, restoration and recovery efforts
  - If they are being yelled at by CEO, other leaders at the same time, they cannot give their best and the company will suffer

Title search: Top 10 Things to Do (or Not Do) in the First 48 Hours

Also available as part of the eCourse
Taking Your Incident Response Plan to the Next Level

First appeared as part of the conference materials for the
2024 Essential Cybersecurity Law session
"Top 10 Things to Do (or Not Do) in the First 48 Hours"