RSAConference2019

San Francisco | March 4–8 | Moscone Center

BETTER.

SESSION ID: AIR-T06

Advancing Incident Response in the Age of New Compliance Requirements

Shawn Henry

President of Services + Chief Security Officer
CrowdStrike

Steve Chabinsky

Global Chair of Data,
Privacy & Cybersecurity
White & Case

SHAWN HENRY

PRESIDENT OF SERVICES + CHIEF SECURITY OFFICER, CROWDSTRIKE

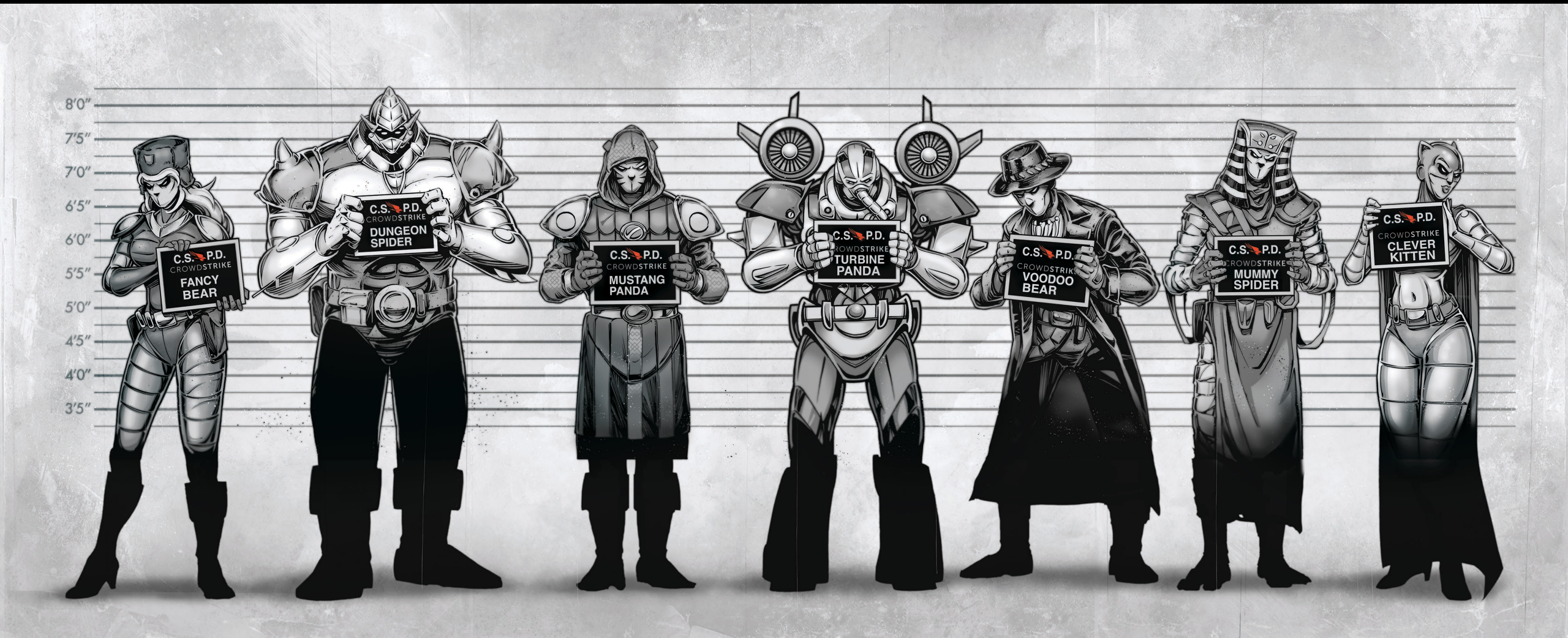
- Leads team of cybersecurity experts to mitigate targeted attacks
- 24 years with the FBI, retiring as Executive Assistant Director

STEVE CHABINSKY

PARTNER + CHAIR OF GLOBAL DATA, PRIVACY & CYBERSECURITY PRACTICE, WHITE & CASE

- Advises global businesses on network security compliance & risk management
- Former Deputy Assistant Director of the FBI Cyber Division

THE REGULATORS THINK YOU CAN HANDLE THEM. DO YOU?



W HY YOU NEED STRONG DETECTION AND RESPONSE

85 Days

AVERAGE ATTACKER DWELL TIME IN 2018

18:48 min

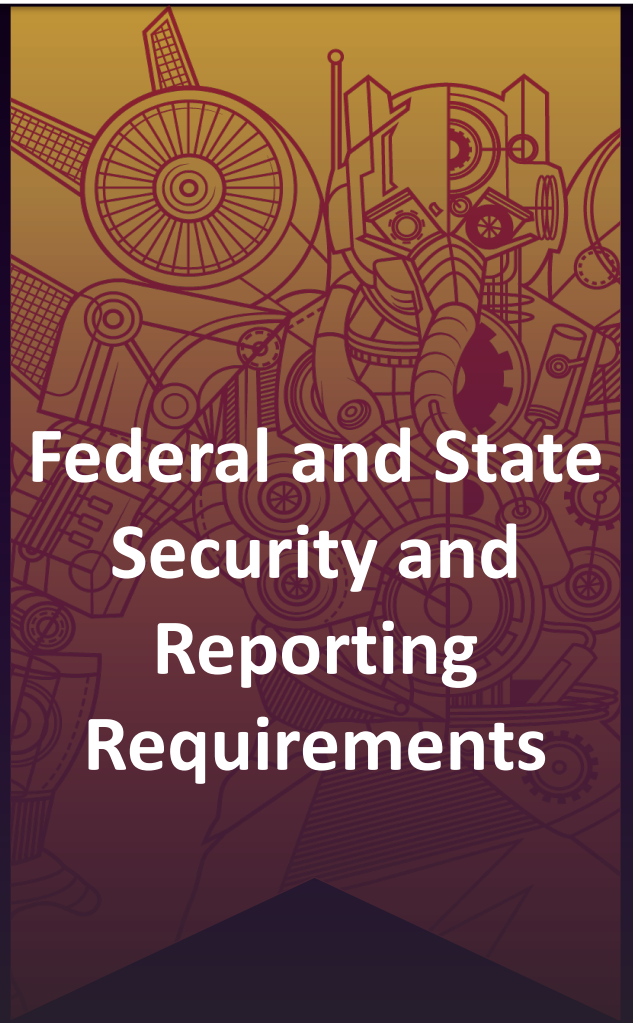
THE TIME IT TAKES A BEAR TO BREAKOUT

Rapid Increase

LIVING-OFF-THE-LAND TECHNIQUES


RETHINKING ORGANIZATIONAL READINESS
STRATEGIC
OPERATIONAL
REPORTING & COMPLIANCE
RISK MANAGEMENT

OUTLINING THE REGULATORY AND CONTRACTUAL LANDSCAPE



RSAConference2019

PART II: DEBUNKING MYTHS & MISCONCEPTIONS

Common Myths

- The breach clock starts ticking when I complete my investigation…
- We'll have my breach investigation details in a few hours…
- I don't need to engage the Board until I discover the breach…
- I don't need IR preparation because I have technology…
- Third party risk isn't my responsibility…

Misconceptions about communicating during/after a breach are the most egregious.

“WE DON’T NEED?”

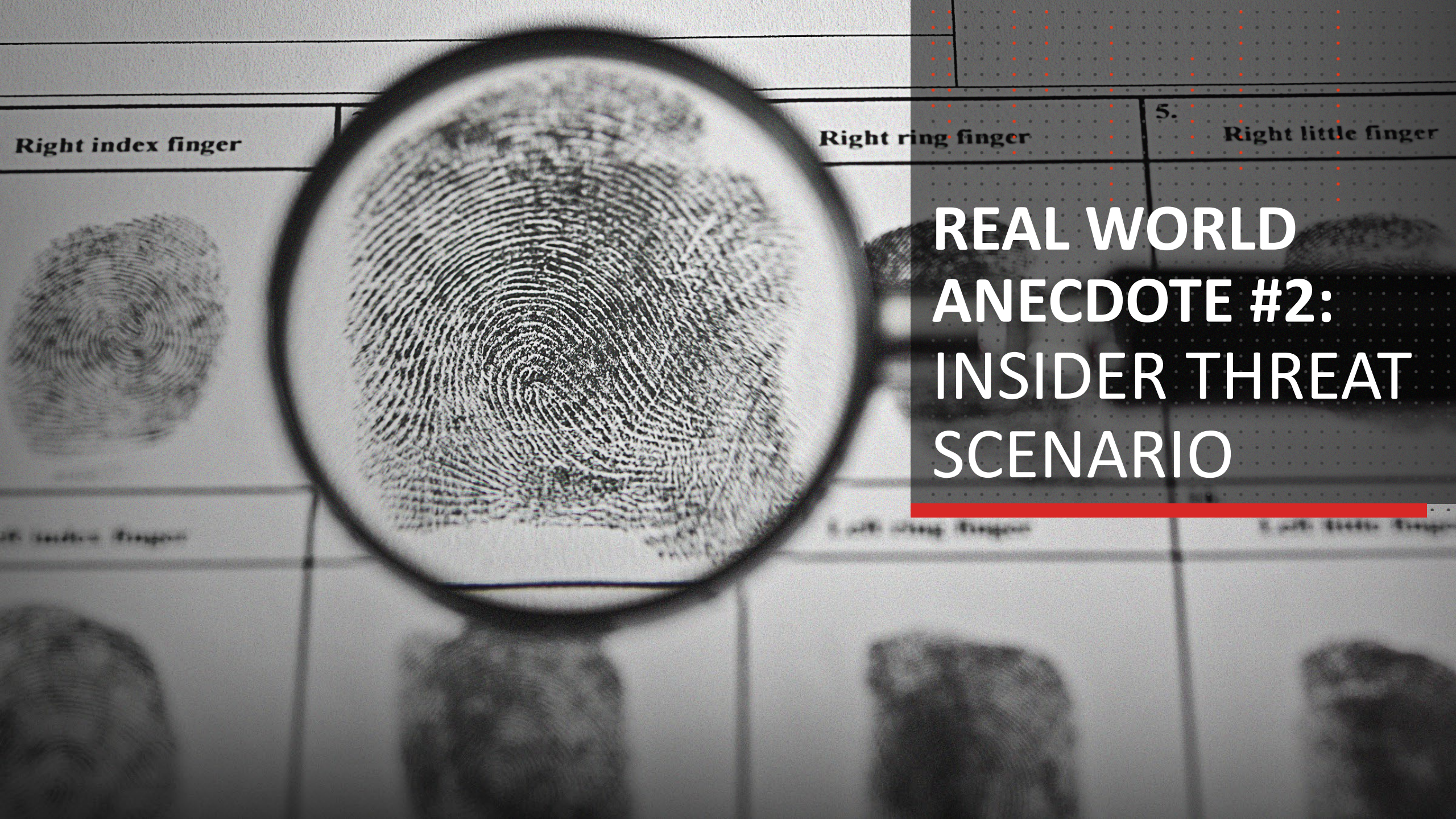
…communication templates

…the comms team in tabletop simulations

…to make statements until we have the full details of the breach

…multiple statements for different audiences

REAL WORLD ANECDOTE #1: MERGERS & ACQUISITIONS



REAL WORLD ANECDOTE #2: INSIDER THREAT SCENARIO

RSAConference2019

PART III: POLLING & WRAP-UP

AUDIENCE POLLING

1. Do you have to disclose an incident if you have clear evidence of data theft?
2. If you suspect data exfiltration has occurred, but don't have definitive evidence to confirm it, are you obligated to report?
3. Do you think your organization is able to meet the 1-10-60 rule?
   (1 min to detect – 10 to investigate – 1 hr to eject the adversary)
4. If you call the FBI when you've experienced a breach, will they provide resources to support your remediation?
5. Under GDPR, must I report a breach within 72 hours only where feasible?

RSAConference2019

THANK YOU

Shawn Henry: shawn@crowdstrike.com
Steve Chabinsky: steven.chabinsky@whitecase.com