Incident Response

Beyond the Technical
10/19/2023

PSG

What are we talking about today?

Agenda

1. Introductions
2. Typical Model
3. 3rd Parties
4. Legal
5. Marketing
6. Finance
7. Take-aways

1 Introductions

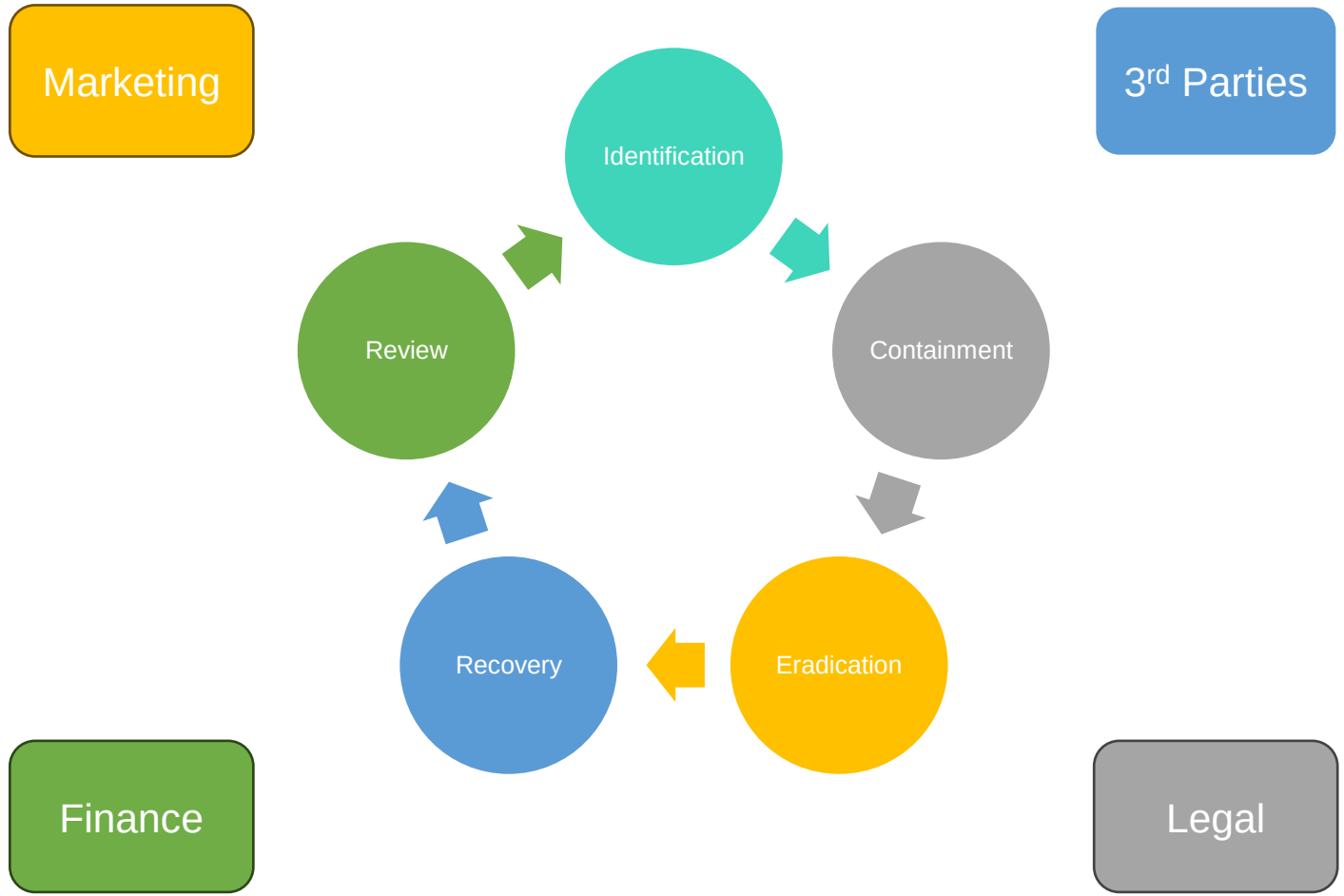
Marc French

CISO & Managing Director

Marc French is the CISO and Managing Director of the Product Security Group. A product guy turned security leader, Marc has more than 30 years in software engineering, product management, and security. Prior to founding PSG, Marc has held a variety of CISO/senior security roles at EMC/RSA, Iron Mountain, Constant Contact, Mimecast and Dun & Bradstreet.

With a passion for growing the future security leaders within infosec, he recently open sourced infosec career ladders and runs a one-on-one mentoring program for students and mid-career professionals.

2 Typical Model - Technical



3rd Parties

In a "Typical Response"

1. Insurance Providers
    - Breach counsel
        - Payment facilitator - more on that later
    - Forensic experts
    - PR firm - more on that later
2. Cloud Providers
    - Production providers
    - Business Systems Providers - Often forgotten
3. Law Enforcement
    - Assisting
    - Collecting
    - Enforcing
        - National Security Letters and such
4. Regulatory
    - Data Protection Authorities
    - FTC
5. Liaison Officer Role

4 Legal

In a "Typical Response"

1. Interfacing
    1. Breach counsel
    2. Law enforcement and regulatory
2. Communications
    - Privileged Communications
    - E-Discovery
3. Declaration
    - Breach or not
4. Reporting
    - Regulatory
    - Shareholder / exchange
    - E-Discovery - yes… called it out again

5 Marketing

In a "Typical Response"

1. Crisis Communications
    - Definition of a crisis
        - BC/DR interface
        - ESG impact
    - PR Firm
2. Monitoring- aka "reputation management"
    - Social Media
    - Press interactions
        - Vishing
3. Security Researchers - Often forgotten

6 Finance

In a "Typical Response"

1. Payments
    - Pre-authorization
        - Sustained operations
            - Food, Lodging, Ubers, etc.
    - Interface with external payment facilitator
        - Ransomware
        - Value of Life
    - Contractor payment
    - Support services for employees
2. Tracking
    - Time
        - Team bonuses
        - Demobilization
    - Services - return to normal operations
3. Insurance Reimbursement

7 Take-aways

- 90% of the incident response plans we see only contain the technical response processes.
- This generally represents maybe 60% of the activities that occur in a mid-to-large scale incident.
- IR plans should represent all activities that will likely be needed in a “typical” incident that an organization will experience. Do not over clock the doc.
- You need to practice **all** these activities in your tabletops.

Reference Note: Take a look at NIMS at FEMA.gov

PSG

THANK YOU

CONTACT INFORMATION

Marc French

mfrench@productsecuritygroup.com

productsecuritygroup.com