

Cyber Security- Trends- Cyber Insurance



Yogi Wright, CPCU, CSR, CISR
Derek Slate, CIC, CSR
Randy Cranfill, MESH, CPSI, CSR

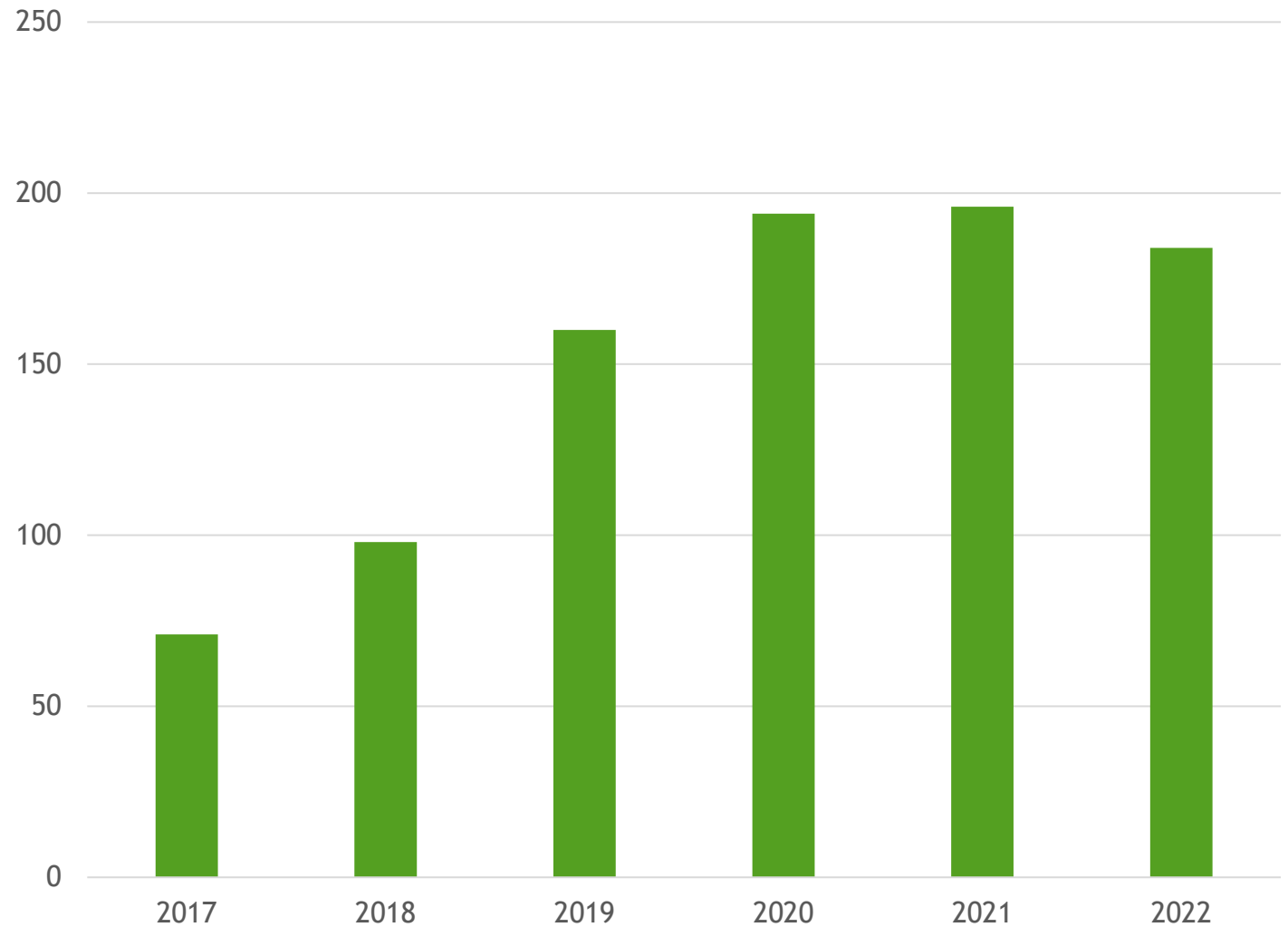
November 08, 2023



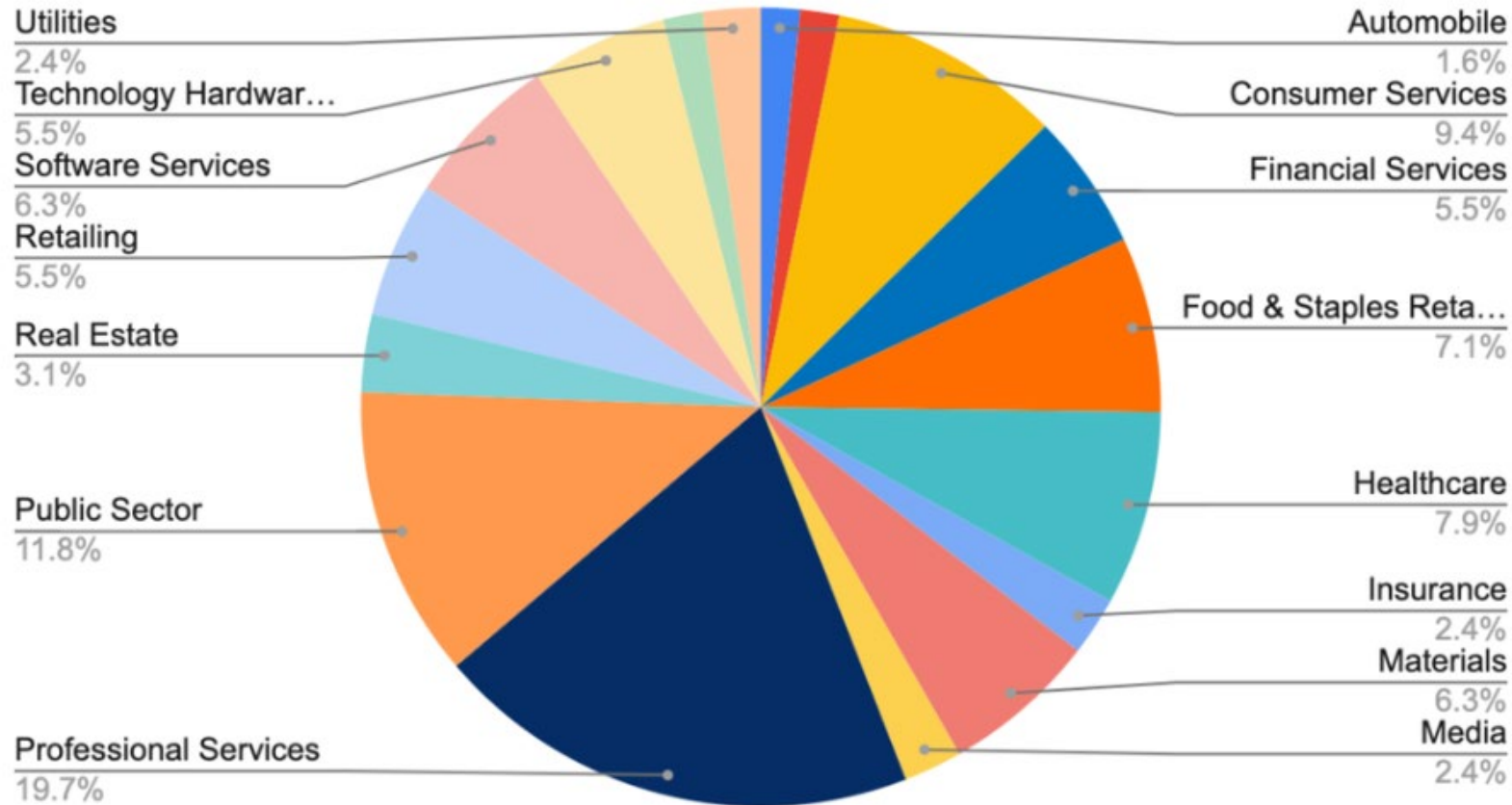
Cyber Claims Data

- 2019-21 – claims spiked to double prior levels
- 2020 – more ransomware than social engineering
- 2021 – equal amounts ransomware and social engineering
- 2022 – 1.5x social engineering claims vs ransomware
- 2023 – level amounts

Total Claims by Year

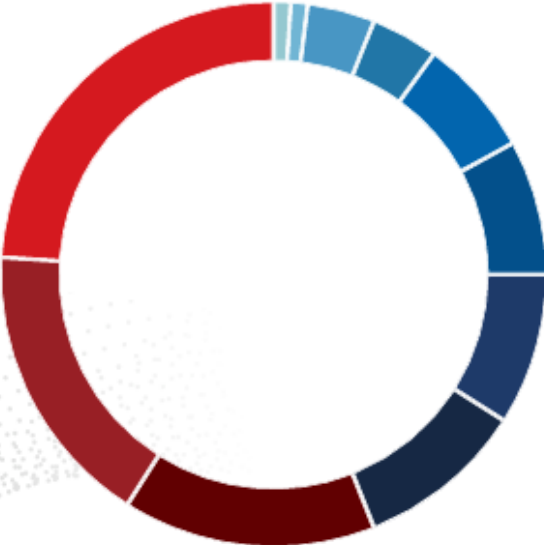


Industries Impacted by Ransomware Q1 2023

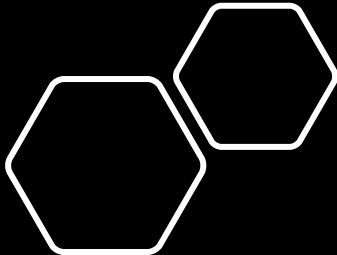


Claims by
Industry

Industries Affected



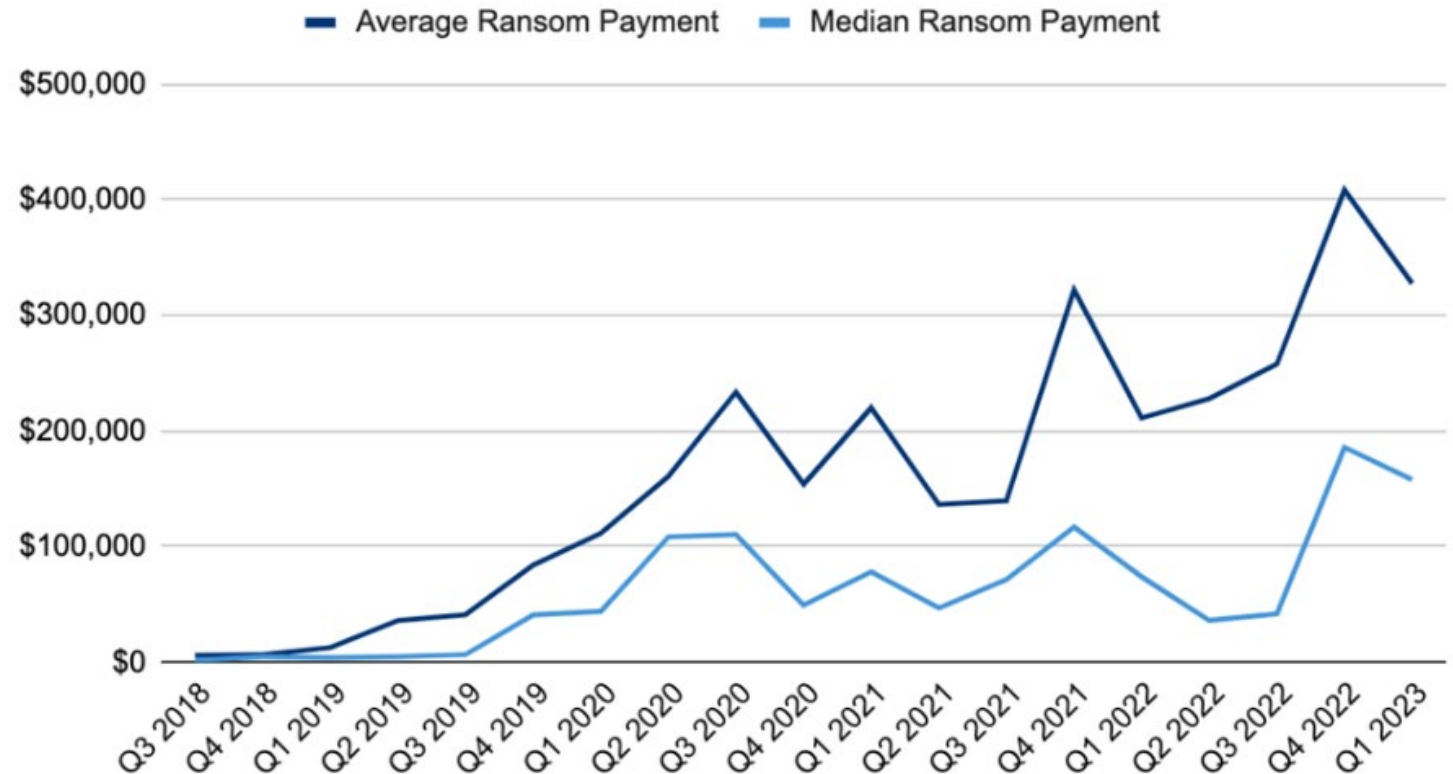
24%	Healthcare <i>(including Biotech & Pharma)</i>	8%	Manufacturing
17%	Finance & Insurance	7%	Government
15%	Business & Professional Services <i>(including Engineering, Transportation, and Managed Service Providers)</i>	4%	Technology
10%	Retail, Restaurant, & Hospitality <i>(including Media & Entertainment)</i>	4%	Non-Profit
9%	Education	1%	Energy
		1%	Other



Payments on the rise

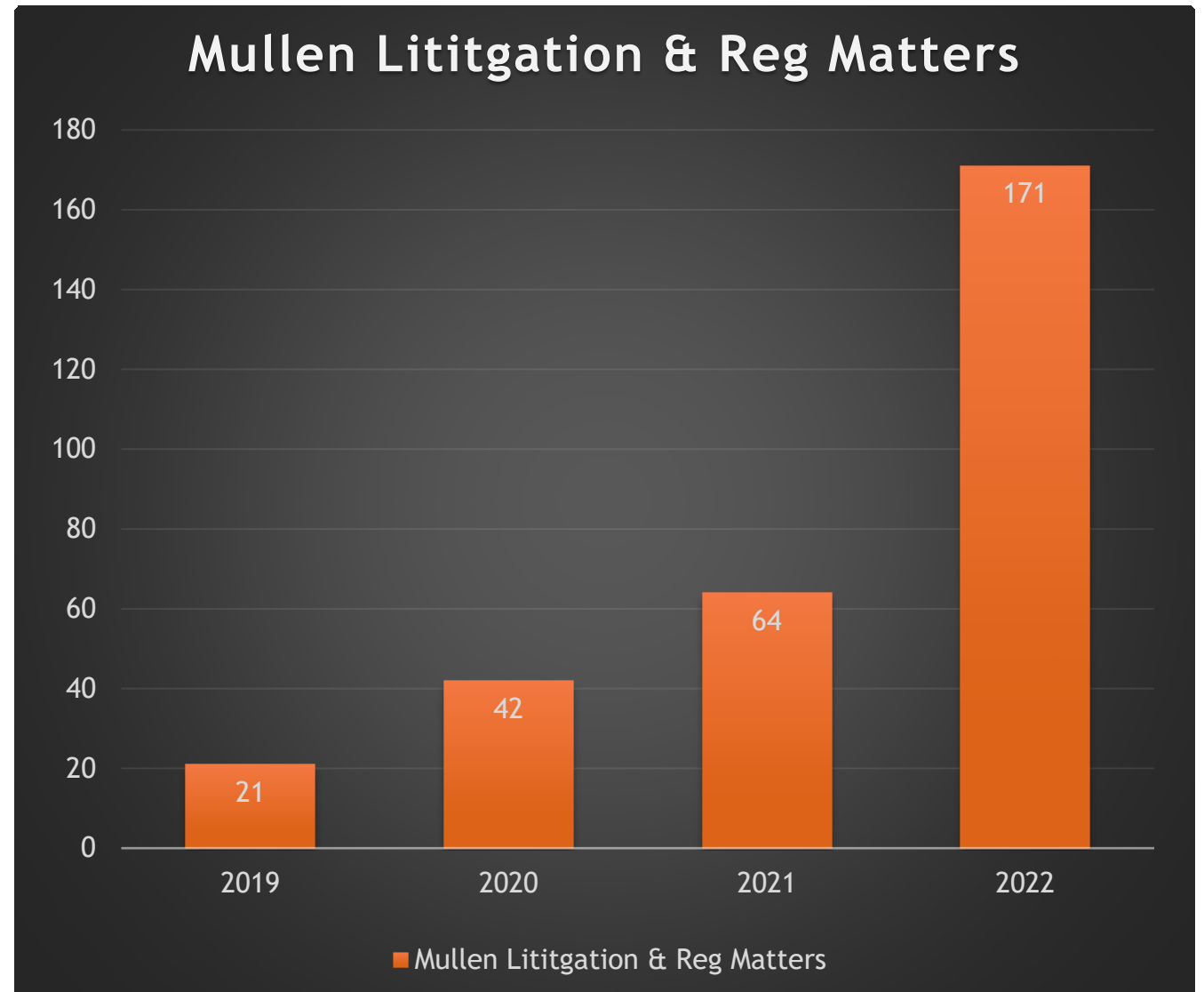
- 45% of initial demands in excess of \$1M
- Mullen average demand of \$2.2M
 - Average payment of \$400k
- Baker average of \$3.7M
 - Average payment of \$600k
- Q1 of 2023 saw 45% of demands resolved via payment (up from mid 30's for most of 2022)

Ransom Payments By Quarter



Rise in Litigation & Regulatory Matters

- Nearly triple number of litigation & reg matters in 22 vs 21
- 42% of matters were in healthcare
- 31% of Baker notifications had a regulatory inquiry, 8.5% had a lawsuit
- As part of ransomware claims
- Privacy Law violations (BIPA!)
- Ad Tracking & Pixel Tracking



The background of the slide features a photograph of a person's hands typing on a laptop keyboard. The person is wearing a light-colored shirt. In the background, other people are seated at tables in what appears to be a meeting or conference room, though they are out of focus. A large, solid green diagonal shape is overlaid on the left side of the image. A semi-transparent orange rectangle is positioned in the center, containing the title text.

Keys to Effective Incident Response Planning



Overview of Incident Response Planning (IRP) Goals and Process



IRP = document that addresses how to effectively handle cybersecurity incidents







Organizations should have an IRP as a matter of legal compliance and/or best practice



Reviewed and updated at least annually

Benefits of Proactive Incident Response Planning

-  Provides a structured and repeatable process
-  Helps identify any gaps in capabilities
-  Based off company's operational realities
-  Test/practice through tabletop exercises

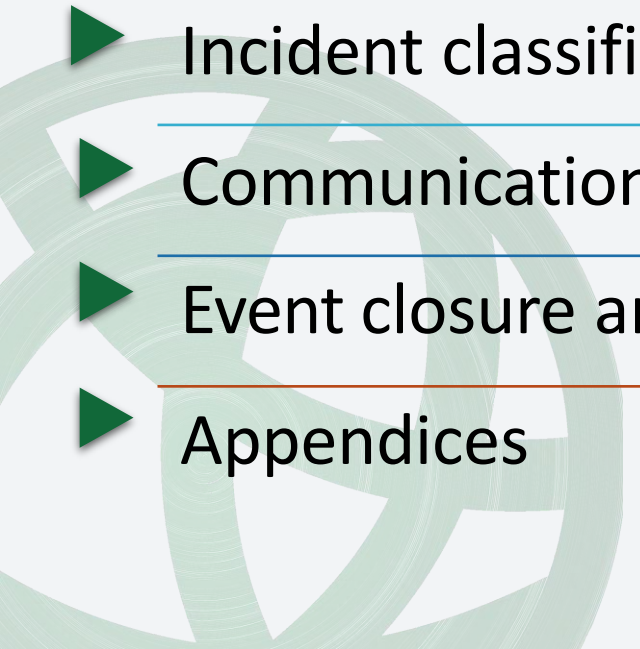
Preparation

Identify the
internal Incident
Response Team
(IRT)

Identify and
Collaborate
with external
resources to
understand
their roles



- Cyber Insurance
- Privacy Counsel
- Incident Response
- Vendors

- 
- ▶ Scope
 - ▶ Definitions of terms
 - ▶ Designation of the IRT members
 - ▶ Identification of potential events
 - ▶ Event escalation
 - ▶ Incident classification & management
 - ▶ Communications guidance
 - ▶ Event closure and lessons learned
 - ▶ Appendices

IRP Components

Scope

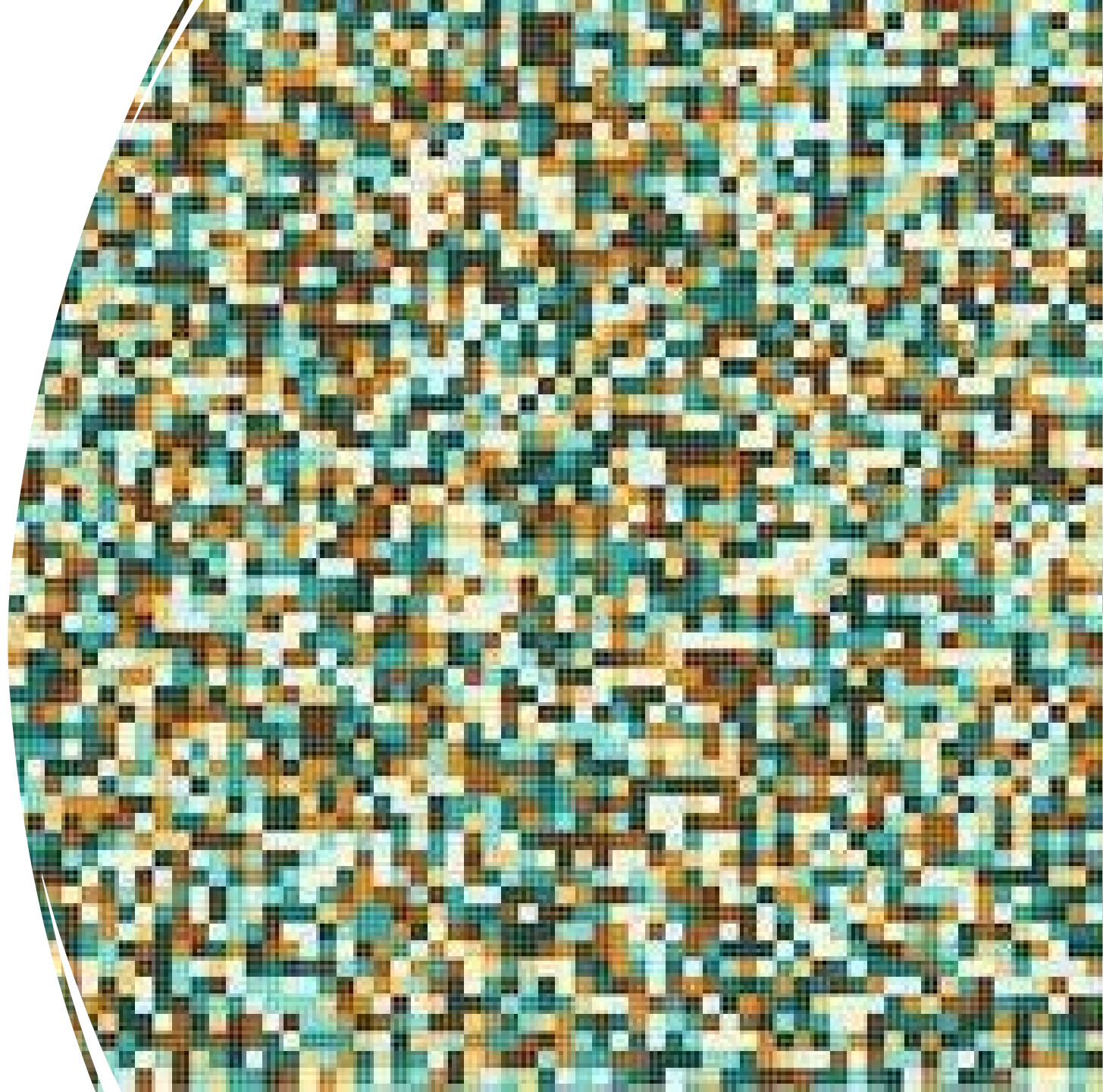
- Cyber IRP's should be specific to **cyber** events
- Cyber IRPs should be holistic and address all threatening events to the organization's system/data/network
- Consider incident-specific playbooks (e.g. ransomware, BEC, PCI, insider threats)

Designation of the Incident Response Team Members

- ▶ Orgs need pre-determined teams, who are responsible for different aspects of the response process
- ▶ Team members should include stakeholders from various departments
- ▶ Team members should have specifically defined roles
- ▶ Designate technical, non-technical, and sub teams for large-scale incidents

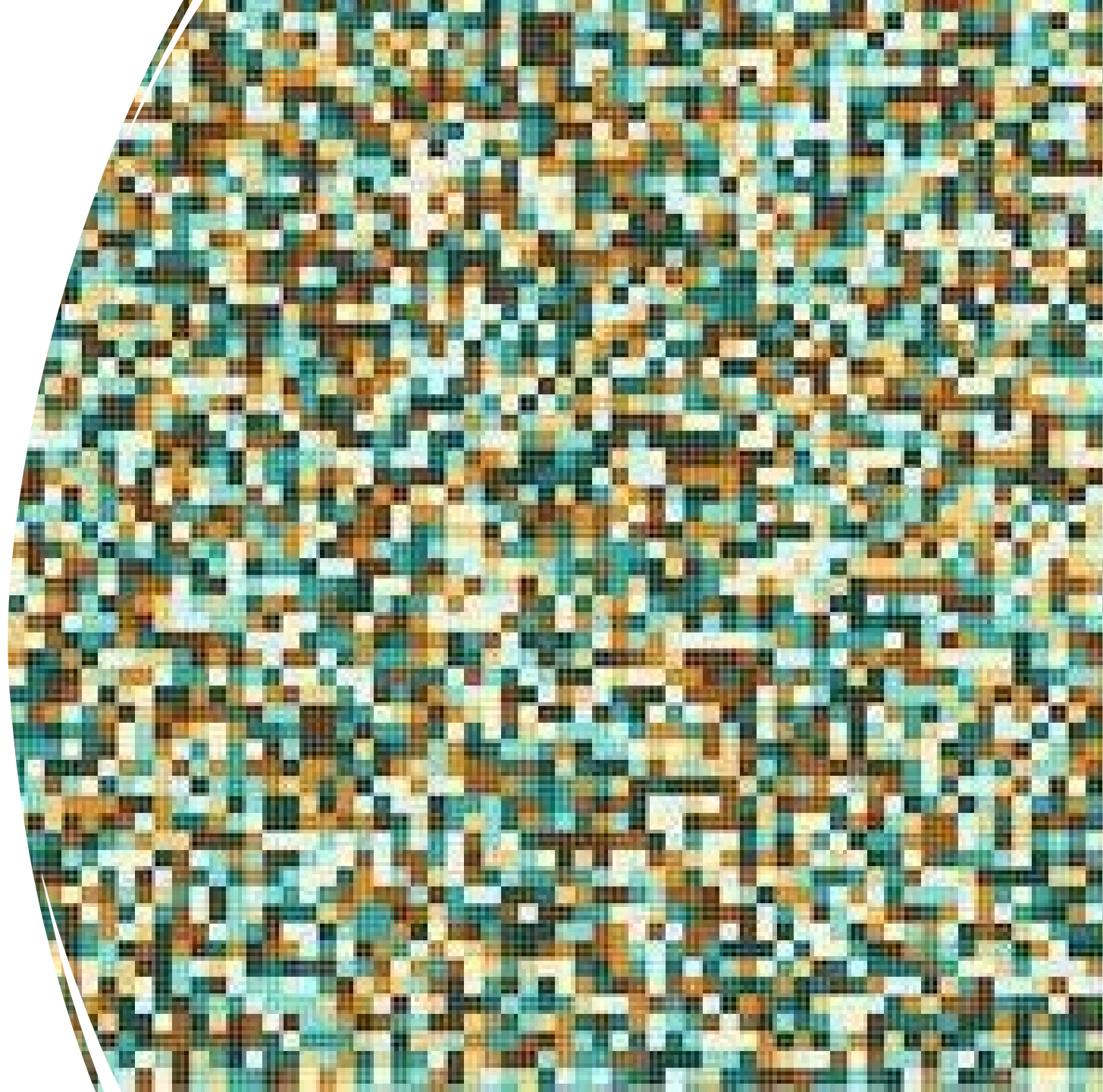
What Is Pixel Tracking?

- Break It Down
 - What's a Pixel?
 - A pixel is a 1×1 graphic that is hidden within web pages and emails
 - How does the Pixel do the Tracking?
 - The pixel loads when a user opens an email or goes to a web page



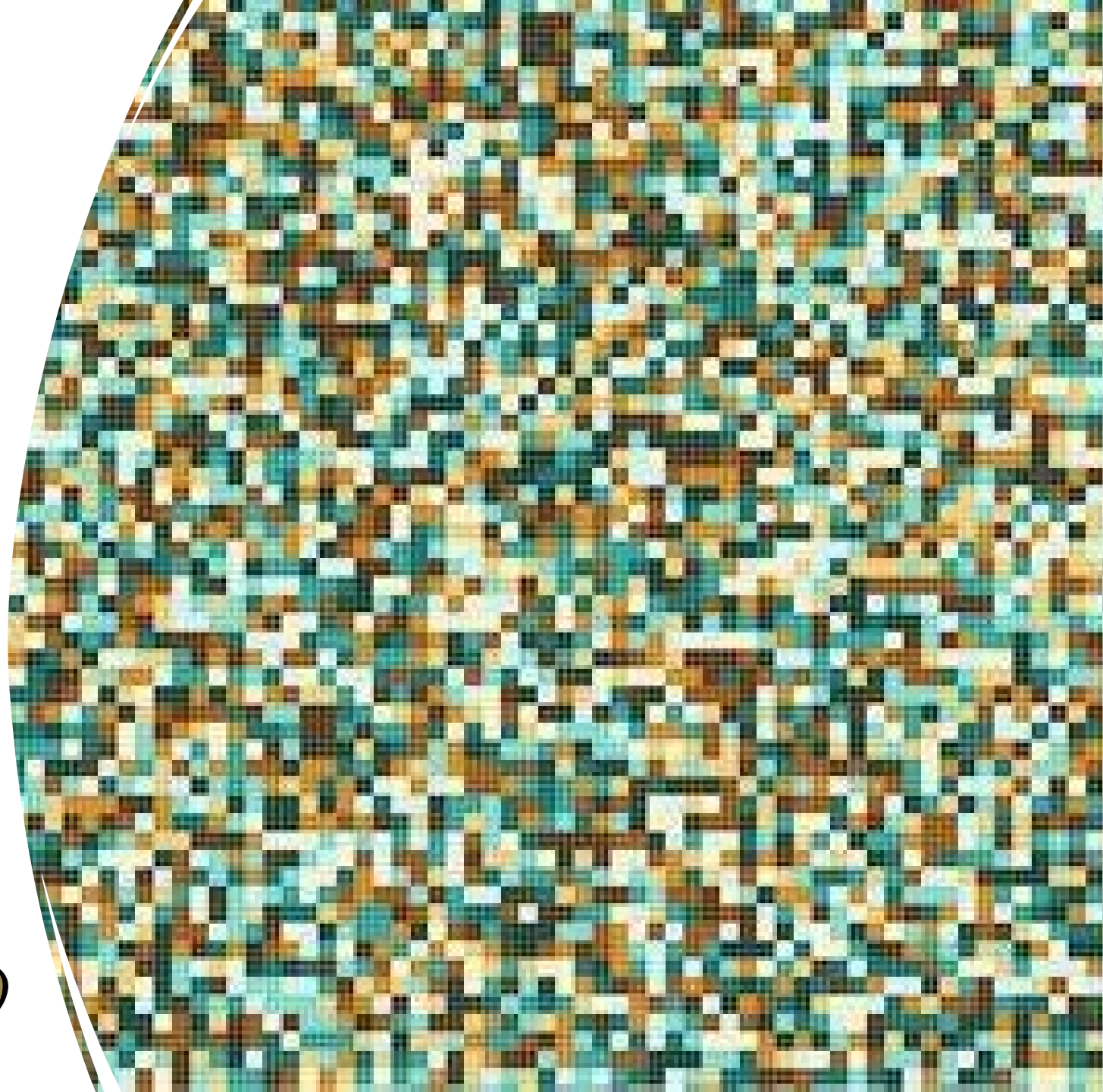
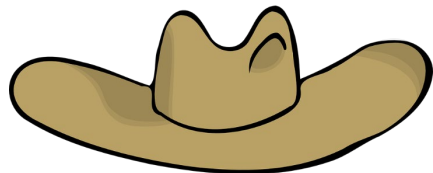
What Does a Pixel Look Like?

- Pixels are typically transparent or colored to blend well with their background
- They are not designed to be seen;
 - Instead, they are intentionally embedded
 - They are camouflaged for digital marketing purposes



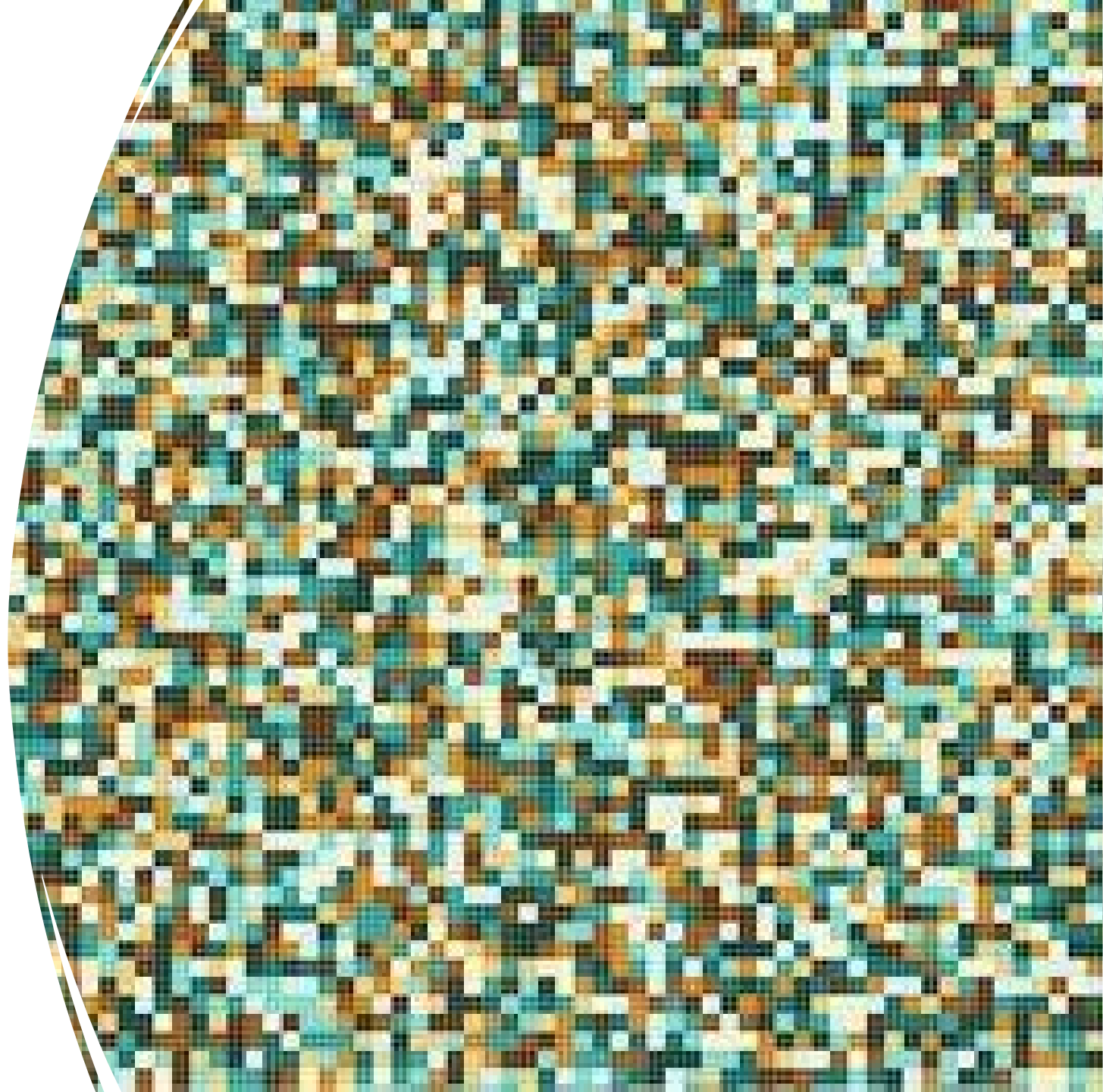
What Is Pixel Tracking?

- Pixel tracking is simply the act of using pixels to collect user data such as their behavior and activities
- Example:
 - You search on a website for a cowboy hat for Thursday night
 - The next time you go to the internet BOOM there is ads for hats



What sort of data can a tracking pixel obtain?

- The type of device the user used
- The type of operating system
- Activities performed during the session
- The user used (browser, mail program, etc.)
- IP address
- What time the user opened the email or visited the website





What Can You Do?

- There are a number of browser extensions that will also block the tracking pixels while alerting you to which emails contain trackers
- *PixelBlock* is a simple Chrome extension that blocks images from loading and displays a red eye at the top of messages when it detects a tracker.
- *Trocker*, which is available for Chrome and Firefox, will show you pixel trackers and identify links that are being tracked

**** Contact your IT Department for more guidance**

Identification of Potential Events

Companies may be notified in various ways, depending on operational structure. Separate workstreams need to be established.

MSSP (Managed Security Services Provider): A resource used for monitoring and management of security devices and systems

SIEM (Security Information Event Management): A tool that helps orgs detect, analyze and respond to security threats

EDR (Endpoint Detection & Response): A tool used for security solution that monitors end-user devices

SOC (Security Operations Center): A resource used for monitoring an organization's entire IT infrastructure

Employees

Third party partners including law enforcement






A background image of a business meeting in a modern office. Several people are seated around a table, some looking at laptops. The image has a teal overlay.

Event Escalation

How to determine if a cyber event becomes a potential incident?

Once identified, who makes the call to declare it an incident and trigger the IRT?

How will the IRT communicate if integrity of communication channels are affected?

-  The significance may be evaluated by the Information Security Team (IST)
-  Decision based on significance of the impact to the organization
-  Incident classification based on impact to the organization
-  IST should confer with the core IRT to evaluate events and classifications
-  An event may be closed by IST because of its lack of effect on data or operations

Escalation Guidelines

Incident Classification

Low Severity

- **Classification:**
 - Cannot be prevented by existing controls, and may involved unauthorized access to data
 - Quickly contained/mitigated using updated/implemented controls
- **Examples:**
 - Loss of company device, installation of remote access tools

Incident Classification *Medium Severity*

- **Classification:**
 - Level 1 plus confirmed material impact to sensitive information or critical information systems
 - Other events that with limited impact that cannot be quickly contained or mitigated
- **Examples:**
 - Insider threat, attempted ransomware attacks, malware, limited network intrusion or business email compromise,

Incident Classification *High Severity*

- **Classification:**
 - Imminent/confirmed unauthorized access, acquisition, or corruption of sensitive information
 - Immediately effect operations or data of external organizations
- **Examples:**
 - Ransomware attack, confirmed data exfiltration, business email compromise, unauthorized access of third-party systems with network connection to company systems

Communications Guidance

- 🌐 **Communication between various IR teams, internal stakeholders, and external parties are necessary**
- 🌐 **Initial communication** should be limited to the IRT, and on a need-to-know basis
- 🌐 **Potential communication to:** employees, executive leadership, Board of Directors, contracting parties/clients/business partners, law enforcement, regulatory authorities
- 🌐 **Tailored communications** based on specific audience
- 🌐 **Communications should be factually based, consistent, accurate**
- 🌐 **Multi-tiered approach** for draft, approval, issuance, and tracking of internal and external communications
- 🌐 **Legal** should always be involved in this process

Event Closure

At the conclusion of an event, there should be a meeting to review performance and lessons learned

Legal should lead and conduct the meeting to maximize protection of attorney-client privilege

Conclusion



Having an IRP is best practice



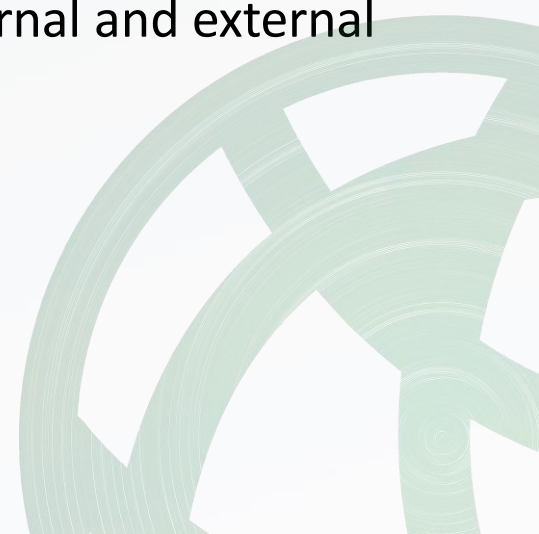
Being prepared for, able to quickly manage, and efficiently and effectively respond to cyber incidents is critical for cyber resilience



Good business practice and helpful for approaching insurance marketplace



Advance planning and collaboration with internal and external resources is critical

A large, faint, light green graphic of a globe is visible in the bottom right corner of the slide.

Source

- **Q1 2023 Coveware**
- **2023 Baker Hostetler Report**
- **INSUREtrust**