2026 Corporate Customer Training
Cybersecurity & Account Takeover

CRI CARR RIGGS & INGRAM
CRIadv.com

This is not a CPA firm.

1

What is Corporate Account Takeover (CATO)?

2

Corporate Account Takeover (CATO)

- Theft of login credentials
- Brute force credential cracking
- Phishing
- Data theft through malware
- Man-in-the-middle attacks

3

Corporate Account Takeover (CATO)

- Criminals gain access to customer finances or data
  - Unauthorized transactions or funds transfer
  - Creation of new/fake online banking users
  - Stolen customer information
- Criminals gain access to bank information

4

How is this accomplished?

- Lack of security
  - Staying logged into Internet Banking (saving credentials within the browser)
  - Sending one time PIN codes to email or text on same machine
- Phishing/malware
  - Exploited devices allow access
  - Sensitive information obtained
- Credential stuffing
- Email compromise
  - Emails appear legitimate
  - Requests seem normal
  - Utilize spoofed/fake email accounts or malware

5

Threat Landscape

6

2025 CrowdStrike Statistics

The average eCrime breakout time fell to **29 minutes** in 2025, a 65% increase in speed from the prior year. The fastest breakout took just **27 seconds**. In one intrusion, data exfiltration began within four minutes of initial access. The window to detect, decide, and respond has narrowed dramatically.

In 2025, evasion was defined by the speed at which adversaries exploit trust. Adversaries operated through valid credentials, trusted identity flows, approved SaaS integrations, and inherited software supply chains. Notably, **82%** of detections were malware-free. Intrusions moved through authorized pathways and trusted systems, blending into normal activity.

Source: CrowdStrike 2026 Global Threat Report

7

2025 CrowdStrike Statistics

Cloud-conscious intrusions rose **37%** in 2025, including a **266%** increase among state-nexus threat actors. Valid account abuse accounted for **35%** of cloud incidents, reinforcing that identity has become central to intrusion. Zero-day exploitation prior to public disclosure increased **42%**, compressing the time between vulnerability discovery and active exploitation.

Source: CrowdStrike 2026 Global Threat Report

8

2025 CrowdStrike Statistics

Source: CrowdStrike 2026 Global Threat Report

9

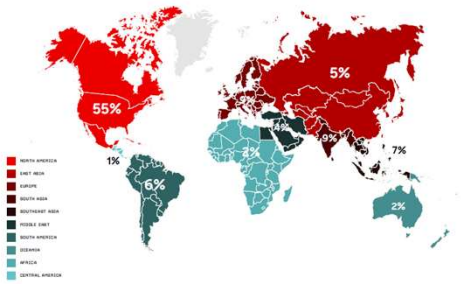
2025 CrowdStrike Statistics

Source: CrowdStrike 2026 Global Threat Report

10

Top 10 Industries Targeted by Interactive Intrusions

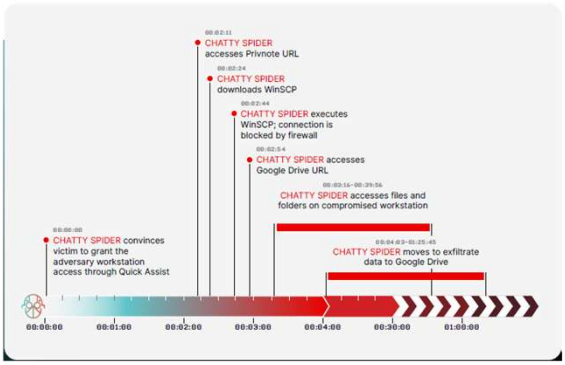
Interactive Intrusions by Region



Source: CrowdStrike 2026 Global Threat Report

11

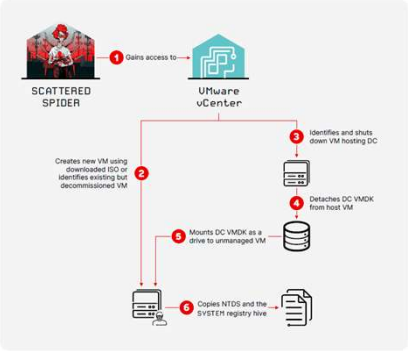
2025 CrowdStrike Statistics - Vishing



Source: CrowdStrike 2026 Global Threat Report

12

2025 CrowdStrike Statistics - Ransomware



Source: CrowdStrike 2026 Global Threat Report

13

2025 CrowdStrike Statistics - Ransomware

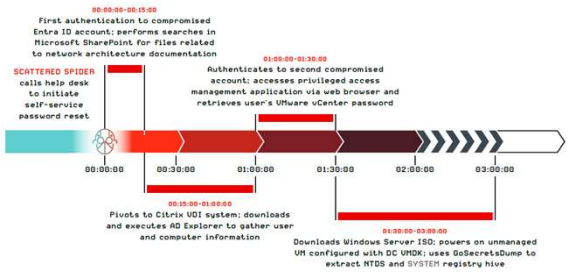


Figure 11. SCATTERED SPIDER dumps NTDS via unmanaged VM in three hours

Source: CrowdStrike 2026 Global Threat Report

14

2025 CrowdStrike Statistics - AI

Source: CrowdStrike 2026 Global Threat Report

15

Biggest Data Breaches in US History

16

Salesforce/Salesloft Drift Campaign –2025

- 1.5 billion people (unconfirmed)
  1. Initial access via GitHub
  2. Reconnaissance
  3. Pivot to Drift environment then stole credentials
  4. Data exfiltration

Source: UpGuard, The 83 Biggest Data Breaches of All Time

17

National Public Data (NPD) – 2023-2024

- Approximately 2.9 billion data records, impacting 1.3 billion individuals
- Exposed data included full names, physical addresses, dates of birth, Social Security numbers (SSNs), phone numbers, and email addresses, posing severe risks of identity theft and fraud.
- The incident led to the collapse of NPD's operations and highlighted a lack of fundamental security measures, such as proper database access controls.

Source: UpGuard, The 83 Biggest Data Breaches of All Time

18

Change Healthcare - 2024

- 145 million records lost
- Customer and patient PII and PHI (names, dates of birth, health insurance information, and potentially Social Security Numbers) compromised
- Ransomware attack through exploitation of known vulnerability (unpatched server)
- Severe impact on medical billing and prescription services nationwide

Source: UpGuard, The 83 Biggest Data Breaches of All Time

19

Snowflake – 2024

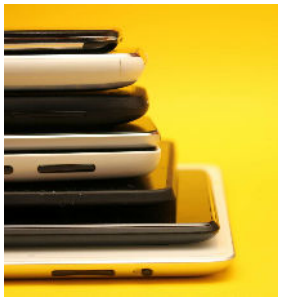
20

MGM Resorts – 2023-2024

21

Stryker – March 11, 2026

- No malware involved
- Remote wipe of employee computers (more than 80,000)
- Possible data exfiltration (still under investigation)
- All done through InTune MDM



22

Baseline Cyber Practices

23

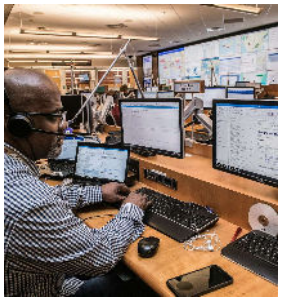
Vendor Management

- New Relationships
  - How do you vet these vendors?
  - Performing risk assessments
  - Reviewing vendor controls
- Existing Vendors
  - Establishing processes to review these vendors according to risk presented to the organization
    - Audit reports
    - Backup and/or disaster recovery (policies and testing)
    - Financial condition
    - Existing contracts
    - Review of controls implemented

24

Incident Response

- Develop procedures
  - Identify
  - Investigate
  - Contain
  - Analyze
  - Recover
- Monitoring for suspicious activities throughout your organization (not just one system)
- Ensure staff know what to do and how to identify



25

User Administration/Authentication

- User Access
  - Access based on least privilege (need to know)
  - Periodic user access reviews
- Authentication Security (Layered controls)
  - Minimum password length and complexity (12-15 characters)
  - Account lockout
  - Inactivity timeout
  - Multi-factor authentication (One-time PIN, token, biometrics, etc.)

26

Email Security

- Encryption for confidential/sensitive information
  - Sending and receiving
- Auto-forwarding disabled
- If not needed, limit or restrict web mail
- Evaluation of links for malicious content

27

Wi-Fi Security

- Ensure properly secured Wi-Fi, including those at home offices (WPA3 encryption)
  - Avoid use of public Wi-Fi. If necessary, use a VPN
- Secure password for access
- Guest network for non-business systems (segregate)
- Keep personal and business devices up to date
- Consider the use of mobile hotspots
- Update wireless access points

28

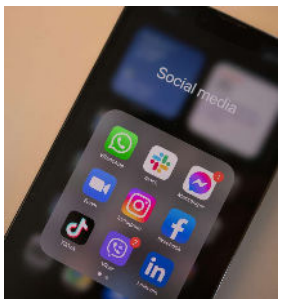
Device Management

- Inventory devices (workstations, laptops, servers, mobile devices, IoT devices)
- Ensure appropriate patch and malware management is implemented (centralized)
  - Include all devices, not just workstations
  - Include applications and operating systems
- Limit local user rights (installing applications and/or browser add-ons, no admin access, etc.)
- Implement web content filtering

29

Social Networking

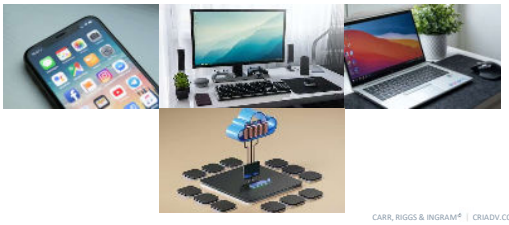
- REMEMBER… Limit what personal information you post
  - Can lead to social engineering attacks (phishing, vishing)
  - Can lead to identity theft
  - Can provide answers to security questions and answers
- Your data is not always private, even when you think it is!



30

Data Security

- Inventory your data
  - Know where your data is located/stored (foreign countries, cloud applications, etc.)
- Determine what type of retention is necessary
- Purge unnecessary data once retention periods are met



31

Remote Access

- VPN, LogMeIn, GoToMyPC
- Increased risk due to increase in end users
- Require proper security measures
  - Authentication controls
  - Prevention of access from unauthorized devices
  - Security of end point devices used to access

32

Shadow IT

- Apps or devices that are used without IT's knowledge
  - Personal or mobile devices
- Rogue cloud services
  - Personal email, document scanning, cloud storage
- Improper authorization

33

Artificial Intelligence

34

Customer and Employee Training

35

Katie Herbert, MBA, CISSP, CISA, CISM
CRI Advisors Senior Manager
KHerbert@CRIadv.com

CRI CARR RIGGS & INGRAM

36