ROCHESTER
SECURITY SUMMIT

ARCTIC
WOLF

Real Risk in Today's Landscape

- Bruce Cheney, Sr. Sales Engineer
- Arctic Wolf Networks

- Bruce Cheney, Sr. Sales Engineer, Arctic Wolf Networks
    - Microsoft MCSE NT 4.0, Windows 2000, Windows 2003
    - Microsoft MCITP Windows Server 2008
    - Microsoft MCTS Exchange, SQL Server, SharePoint
    - Citrix Certified Enterprise Engineer PS 4.5
    - CompTIA Sec+, Net+, A+
    - Certified SCRUM Master
- Penetration Tester and Cybersecurity Consultant
- Independent Consultant for NY State Agencies
- Master Technical Trainer, Courseware and Exam Author

Agenda

- **How Did We Get Here?**
- **What is the Real Risk?**
- **The Dark Web**
- **Cyber Risk By The Numbers**
- **Who is doing this?**
- **Dark Web Data Leaks**
- **What Can You Do?**

How did we get here?

What is the Real Risk?

What are the Real Risks?

What could happen if the Bad Actors get in?

- Business Email Compromise

- Ransomware
- Data Deletion
- Data Exfiltration
  - Dark Web Data Leaks

- SEC Reporting
- Employee Harassment
- Investor Notification

Who is doing this?

Nation-State Adversaries

Cybercrime Groups and The Dark Web

What is the Dark Web?

Surface Web (4%)

Google, BING, Yahoo, Facebook, Wikipedia, Amazon, eBay, Disney, CNN, Reddit

Deep Web (90%)

Medical Records, Government Resources, Financial Records, Legal Records, Patent Data, Academic Info

Dark Web (6%)

TOR Encrypted Sites (.onion), Hidden Marketplaces, Drug Trafficking, Illegal Services, Political Protests

CLOP^

The CLOP^ ransomware group, active since early 2019, is known for its sophisticated attacks and multi-layered extortion tactics. They are linked to TA505.

They target high-profile organizations worldwide, often using large-scale phishing campaigns to gain access to networks. Once inside, they steal sensitive data in addition to encrypting it with ransomware. They then threaten to publish the stolen data if the ransom isn't paid, applying significant pressure on victims.

CLOP^ is a significant threat due to their ability to disrupt operations and damage reputations.

Redacted due to sensitive nature of leaked data.

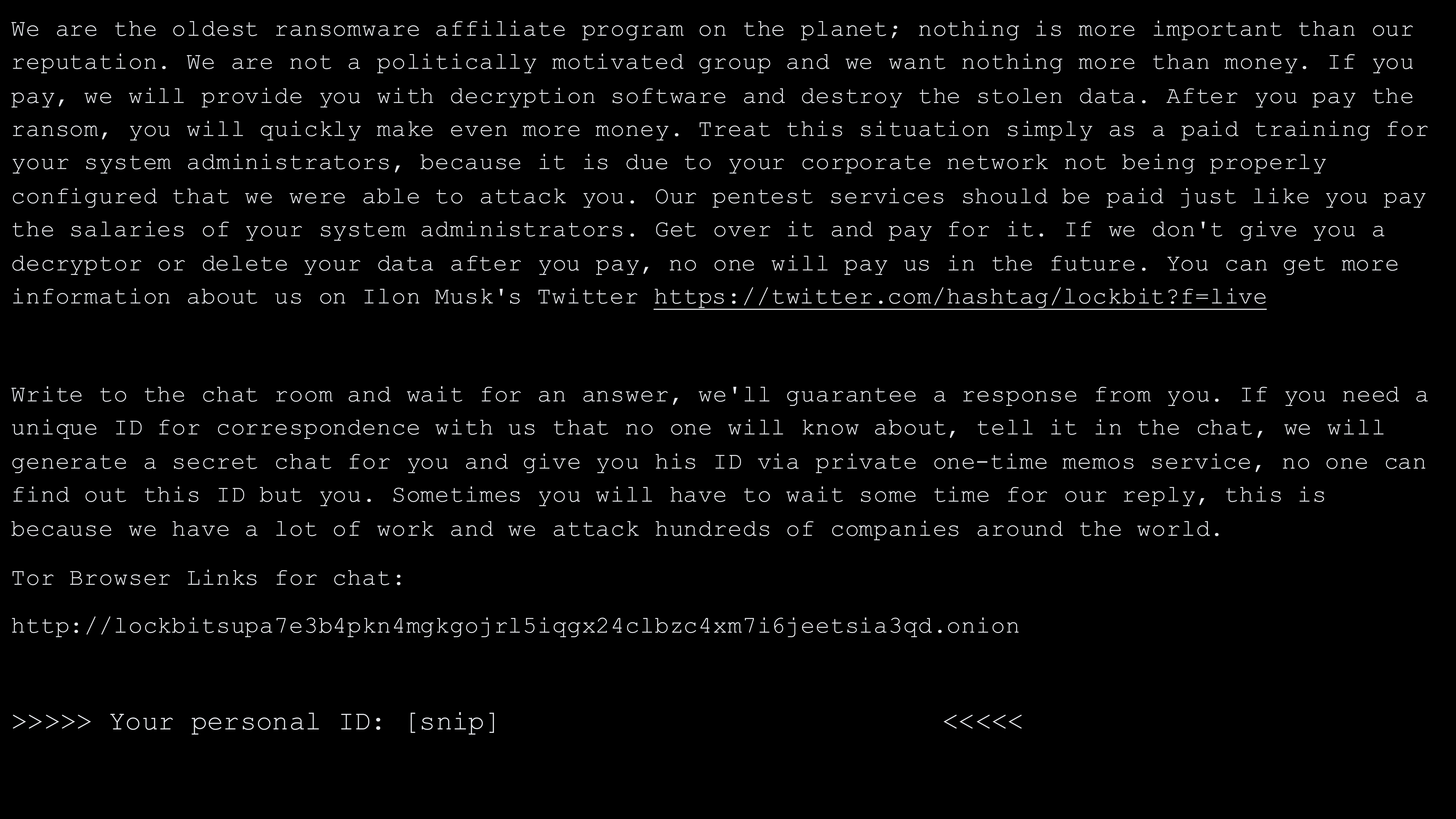
LockBit

The Lockbit ransomware group, active since September 2019, is a highly sophisticated RaaS Operation. They operate with a decentralized affiliate model.

Known for its speed, LockBit can encrypt entire networks in minutes using tools like PDQ Deploy, PsExec, and custom scripts—often achieving full deployment in under 3 hours.

Lockbit uses persistent evolution and evasion techniques. The group frequently updates its malware to bypass security tools, employs double extortion tactics (data theft + encryption), and targets high-value organizations across sectors.

```
~~~ LockBit 3.0 the world's fastest and most stable ransomware from 2019~~~


>>>>> Your data is stolen and encrypted.


If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep
in mind that once your data appears on our leak site, it could be bought by your
competitors at any second, so don't hesitate for a long time. The sooner you pay the
ransom, the sooner your company will be safe.

Tor Browser Links:

http://lockbitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead.onion

http://lockbitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd.onion

>>>>> What guarantee is there that we won't cheat you?
```



We are the oldest ransomware affiliate program on the planet; nothing is more important than our reputation. We are not a politically motivated group and we want nothing more than money. If you pay, we will provide you with decryption software and destroy the stolen data. After you pay the ransom, you will quickly make even more money. Treat this situation simply as a paid training for your system administrators, because it is due to your corporate network not being properly configured that we were able to attack you. Our pentest services should be paid just like you pay the salaries of your system administrators. Get over it and pay for it. If we don't give you a decryptor or delete your data after you pay, no one will pay us in the future. You can get more information about us on Ilon Musk's Twitter https://twitter.com/hashtag/lockbit?f=live

Write to the chat room and wait for an answer, we'll guarantee a response from you. If you need a unique ID for correspondence with us that no one will know about, tell it in the chat, we will generate a secret chat for you and give you his ID via private one-time memos service, no one can find out this ID but you. Sometimes you will have to wait some time for our reply, this is because we have a lot of work and we attack hundreds of companies around the world.

Tor Browser Links for chat:

http://lockbitsupa7e3b4pkn4mgkgojrl5iqgx24clbzc4xm7i6jeetsia3qd.onion

```
>>>>> Your personal ID: [snip]                              <<<<<
```

What Happened Here?

1. Intial Access via Malware Impersonation
2. Rapid Privilege Escalation (SystemBC and GhostSOCKS)
3. Persistence and Credential Harvesting (SharpView)
4. Lateral Movement to Critical Servers (Cobalt Strike)
5. Defensive Evasion via GPO
6. Sensitive Data Discovery
7. Data Exfiltration (16 hours-RClone)
8. Ransomware Deployment using PsExec, BITSAdmin, and WMI.
9. Time to Ransomware (239 hours-11 Days)

Redacted due to sensitive nature of leaked data.

Vice Society

Vice Society appeared in mid-2021 and is known for disproportionately targeting the education, healthcare, and manufacturing sectors, often exploiting vulnerabilities like PrintNightmare to gain initial access.

The group uses double extortion, stealing sensitive data before encrypting systems. If ransom demands (often exceeding $1 million) aren't met, they threaten to publish the data on leak site.

Unlike many ransomware groups, Vice Society does not operate as a RaaS. They conduct their own intrusions using tools like Cobalt Strike, Mimikatz, and SystemBC, and have developed custom ransomware variants for stronger encryption

Redacted due to sensitive nature of leaked data.

Cloak

Cloak emerged in late 2022, using Initial Access Brokers and social engineering to infiltrate networks.

Payloads are delivered via VHDs and disguised installers, often mimicking Windows updates. They also modify registry settings to restrict user actions and ensure persistence. The group disables antivirus, backup, and database services to maximize disruption.

Cloak ransom payments are extremely high- around 95%.

Redacted due to sensitive nature of leaked data.

What Can You Do?

Be Prepared, Have a Plan, Be Ready To Execute

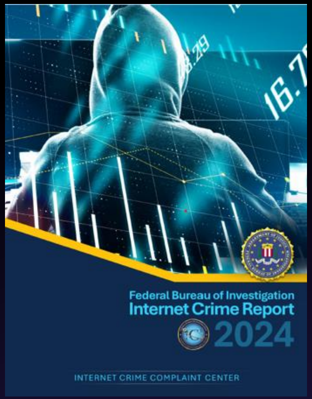
- Follow a Framework→ i.e., NIST CSF
- Assess Your Exposure, Not everyone faces the same risks. Know yourself…
- Minimize your Attack Surface
- Monitor and Alert 24x7 (MDR)
- Train your users
- Create and Test an IR Plan
- Implement Zero Trust
- Share and Collaborate

- Continue to Execute the Basics

MFA
Patching
Backups
Change Control
Password Management
Secure WIFI
DNS Security

EPP
DLP
Limit User Privilege
Use Encryption
Network Segmentation
Control Removable Media
Email Security

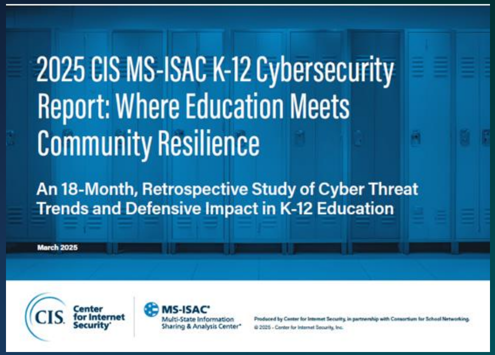
Cyber Risk by the Numbers…


Federal Bureau of Investigation
Internet Crime Report
2024
INTERNET CRIME COMPLAINT CENTER

2025 Data Breach Investigations Report
verizon business

ARCTIC WOLF
ARCTIC WOLF
2025
THREAT REPORT

ARCTIC WOLF LABS
ARCTIC WOLF LABS
2025
PREDICTIONS


2025 CIS MS-ISAC K-12 Cybersecurity Report: Where Education Meets Community Resilience

An 18-Month, Retrospective Study of Cyber Threat Trends and Defensive Impact in K-12 Education

March 2025

CIS Center for Internet Security

MS-ISAC Multi-State Information Sharing & Analysis Center

Produced by Center for Internet Security, in partnership with Consortium for School Networking.
© 2025 - Center for Internet Security, Inc.

Consolidated Insights – Unified Lessons

- The Threat Landscape is Dominated by a Few Core Attack Types
  - **Ransomware, BEC, and intrusions** remain the most common and costly attack types
  - **Ransomware prevalence** rose in most reports, but **ransom payment rates fell**, showing defensive gains.
- Humans Remain the Primary Attack Surface
  - Phishing, vishing, and social engineering dominate initial access vectors
  - K-12 and small businesses are especially vulnerable due to training gaps and operational stress.
- Monetary Losses Are Staggering and Widespread
  - $16.6B in reported U.S. cybercrime losses
  - **Access markets**, **infostealers**, and **persistent access** are monetized rapidly.
  - The financial toll of cybercrime isn't limited to ransoms – it's also in **lost operations**, **incident recovery**, and **community disruption**.

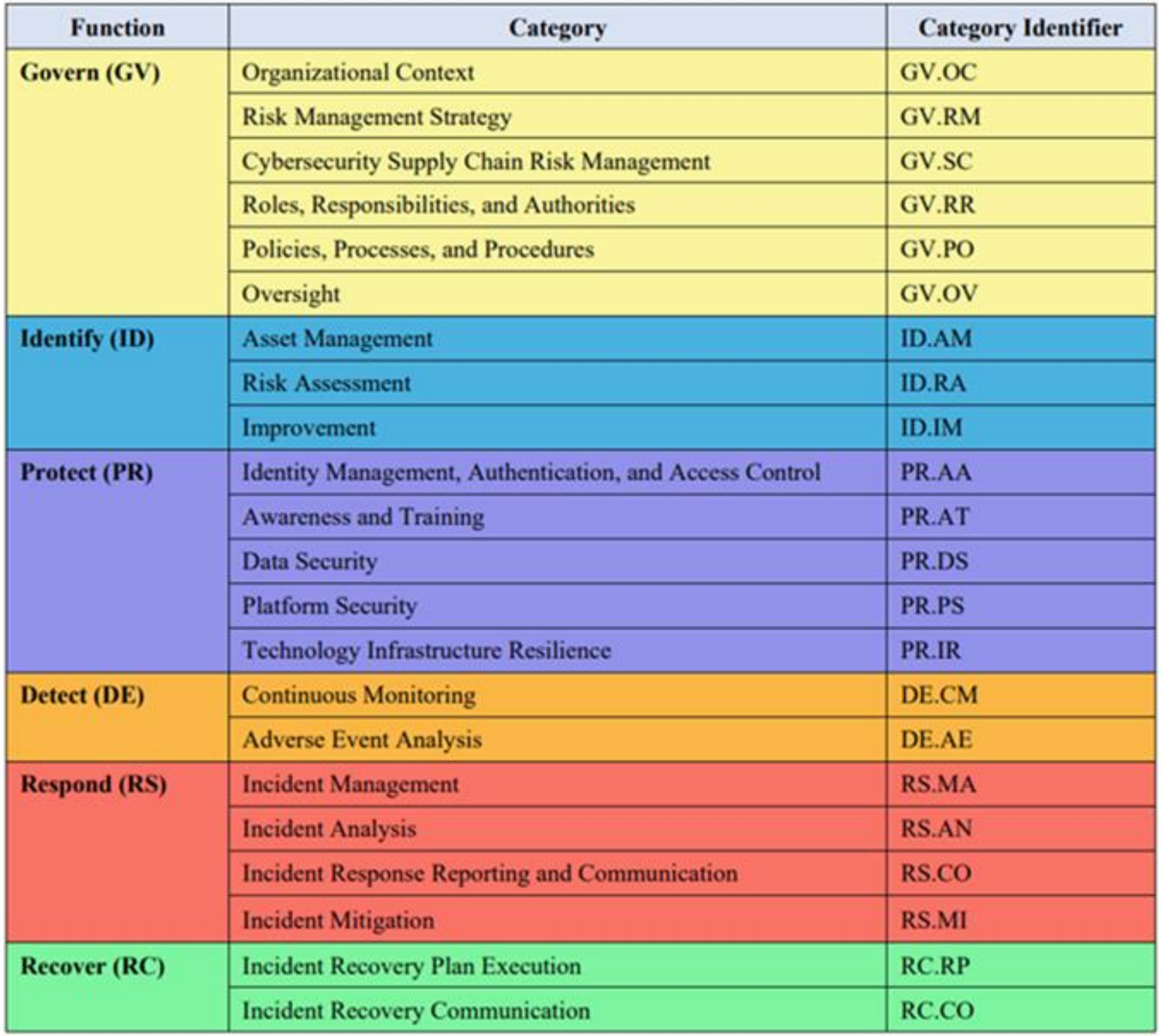
Consolidated Insights – Unified Lessons (cont.)

- Sector-Specific Threats and Timed Exploitations are growing
  - **Manufacturing, Education, Healthcare, and Finance** were top targets across reports.
  - Threat actors tailor their techniques to sector-specific pressures – knowing when and where victims are most vulnerable.
    - Exam weeks, holidays, maintenance periods
  - **Critical Infrastructure** (energy, healthcare, government) targeted for both extortion and hybrid warfare
- Defenders Must Focus on Fundamentals + Automation
  - Common root causes: **Unsecured RDP**, **poor VPN configurations**, **orphaned IAM accounts**, and **lack of segmentation**.
  - Fundamentals still win: Patch aggressively, monitor identities, segment networks, and automate detection.

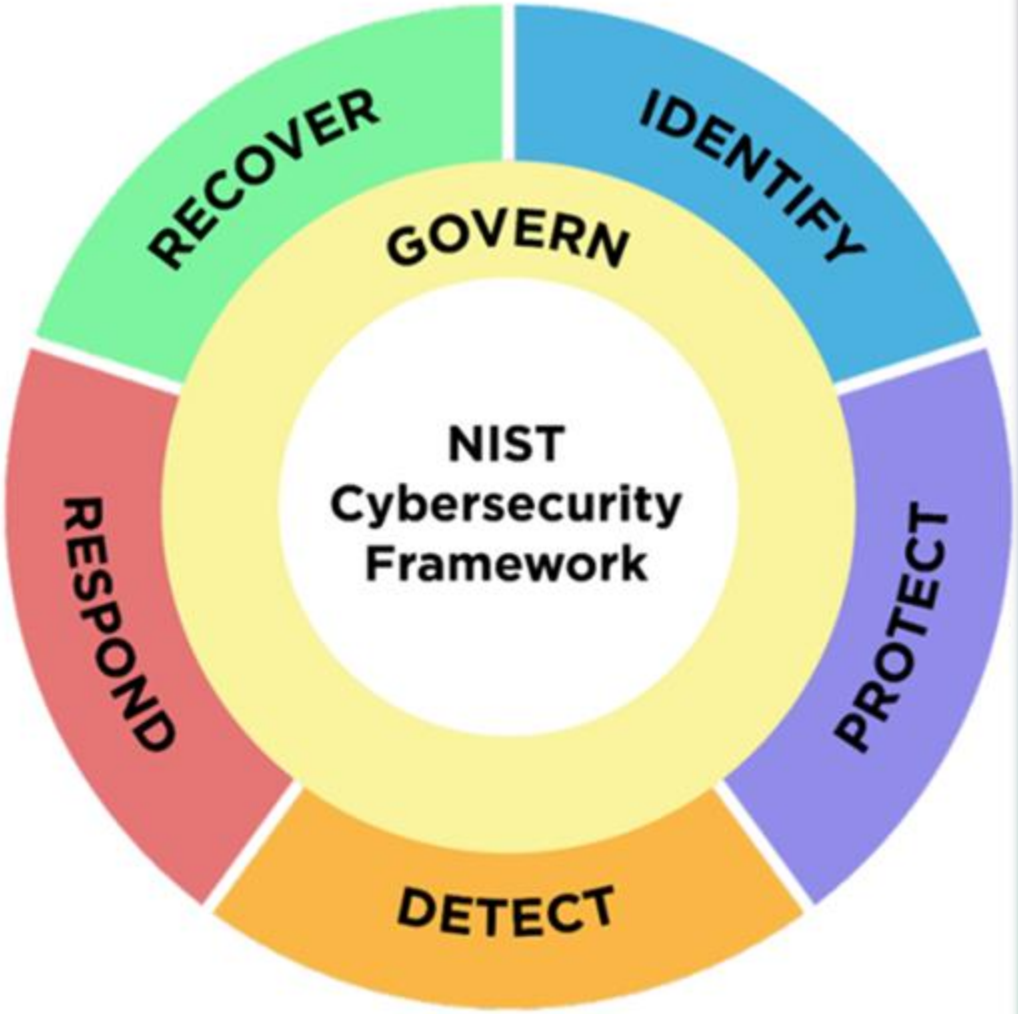
Consolidated Insights – Unified Lessons (cont.)

- Credential & Identity Abuse is the New Perimeter
  - Valid credential use now **surpasses malware** in many cases
  - Identity and access misconfigurations drive **35%+** of cloud breaches
  - GenAI, phishing kits, and infostealers amplify credential abuse effectiveness
- Third Parties and SaaS Platforms Are Growing Attack Vectors
  - **Vendor security** is now a core operational risk, not just a compliance concern
  - SaaS platforms like Snowflake and CDK Global targeted for their integration with many clients
- Collaboration and Culture Matter
  - The **shift from blaming users** to **empowering them** with training, open communication, and feedback loops is essential.
  - Resilience isn't just technical – it's organizational. Community collaboration and internal empowerment reduce risk across the board.

NIST Cybersecurity Framework 2.0

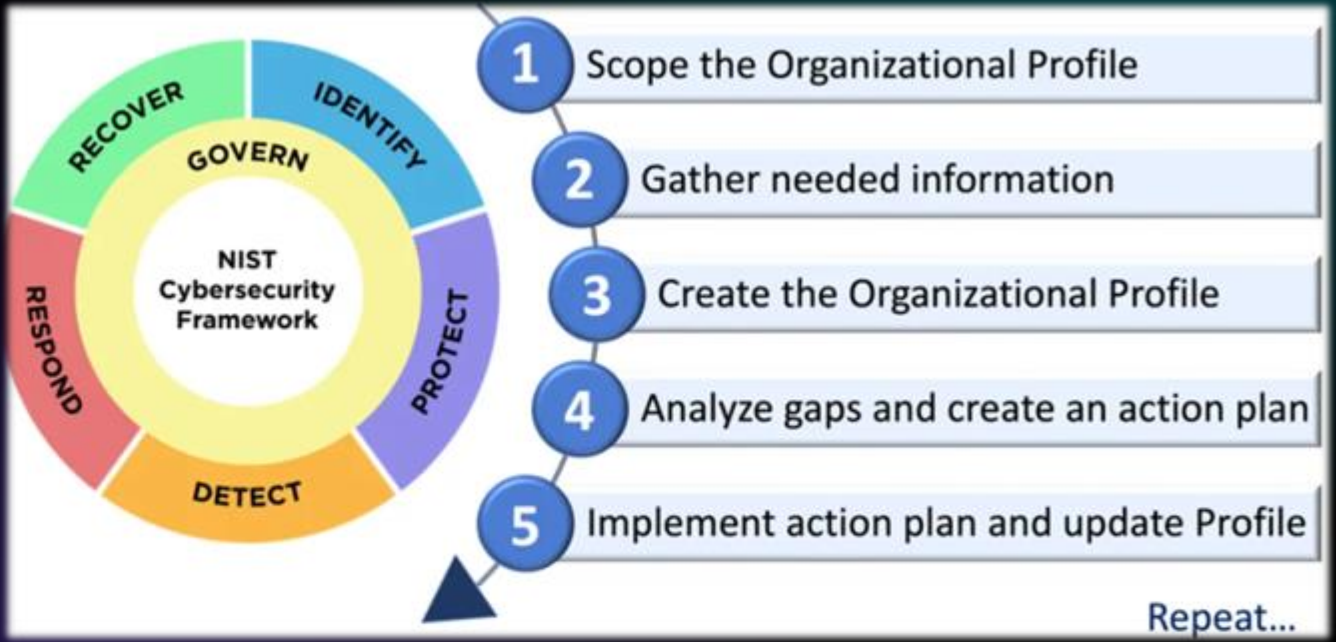


Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Cybersecurity Supply Chain Risk Management	GV.SC
	Roles, Responsibilities, and Authorities	GV.RR
	Policies, Processes, and Procedures	GV.PO
	Oversight	GV.OV
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO



NIST Cybersecurity Framework 2.0

Organizational Profile



1. Scope the Organizational Profile
2. Gather needed information
3. Create the Organizational Profile
4. Analyze gaps and create an action plan
5. Implement action plan and update Profile

Repeat...

Questions?

Bruce.Cheney@ArcticWolf.com