





**CIBERSEGURIDAD EN EL
SECTOR ASEGURADOR:
MEDIDAS Y CONTROLES PARA
GESTIONAR Y PROTEGER LA
INFORMACIÓN DE LOS
ASEGURADOS DERIVADO DE
ATAQUES CIBERNÉTICOS.**

Lcdo. Alexander S. Adams Vega
Comisionado de Seguros de Puerto Rico



Oficina del Comisionado de Seguros de Puerto Rico

Threat actors | Overview

| | |
|--|--|
|  <p>Nation-state linked</p> | <ul style="list-style-type: none"> Motivation — Political, Espionage, Financial Likelihood — Likely, Significant long-term impact Top Actors — BlackTech, Volt Typhoon, Maui ransomware, Lazarus Group |
|  <p>Cybercriminals</p> | <ul style="list-style-type: none"> Motivation — Financial Likelihood — Likely, Significant immediate impact Top Actors — LockBit, ALPHV/Blackcat, Play Ransomware, Akira Ransomware |
|  <p>Hacktivists</p> | <ul style="list-style-type: none"> Motivation — Political Likelihood — Roughly even chance, Moderate impact Top Actors — SiegedSec, Five Families (Blackforums, GhostSec, SiegedSec, Stormous, and ThreatSec) |
|  <p>Insider threat</p> | <ul style="list-style-type: none"> Motivation — Financial, Revenge, Fear (blackmailed) Likelihood — Malicious: Roughly even chance, Severe impact Unintentional: Likely, Significant impact Top Actors — "bronzegods"; "I_Deleter"; "neboltay"; "jolbit08"; "lies"; "Enony"; |



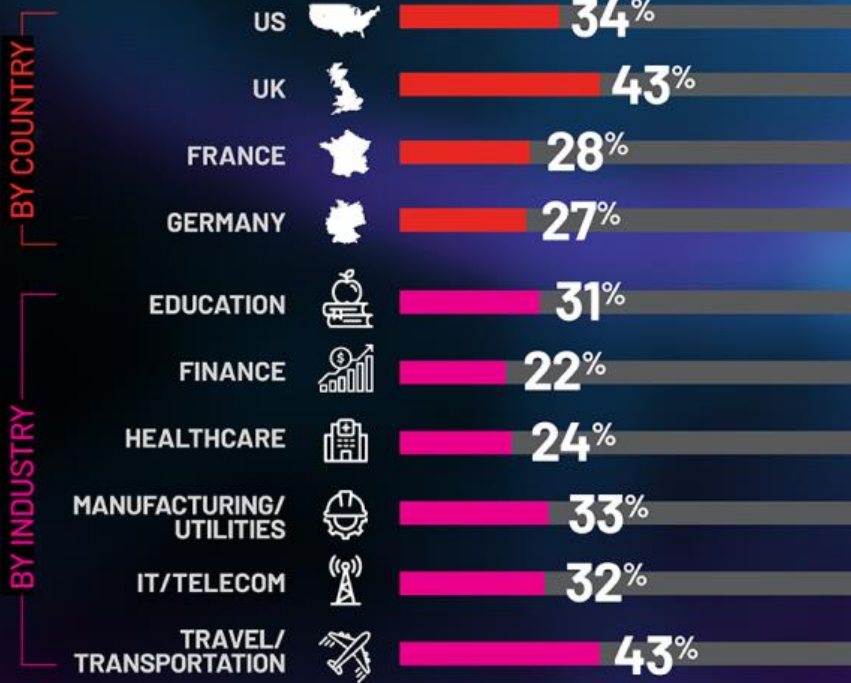
Ransomware

BY THE NUMBERS

Despite meeting attackers' ransom demands,

35%

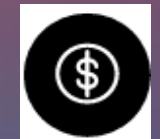
of companies that paid either **didn't receive decryption keys** or **received corrupted keys**.



74%-of the victims were attacked not once, but several times.



87%-of the attacks caused some level of disruption.



78% -that suffered a "ransomware" attack paid a ransom.

Ransomware

BY THE NUMBERS

87%

of attacks caused business disruption, even for those that paid ransom



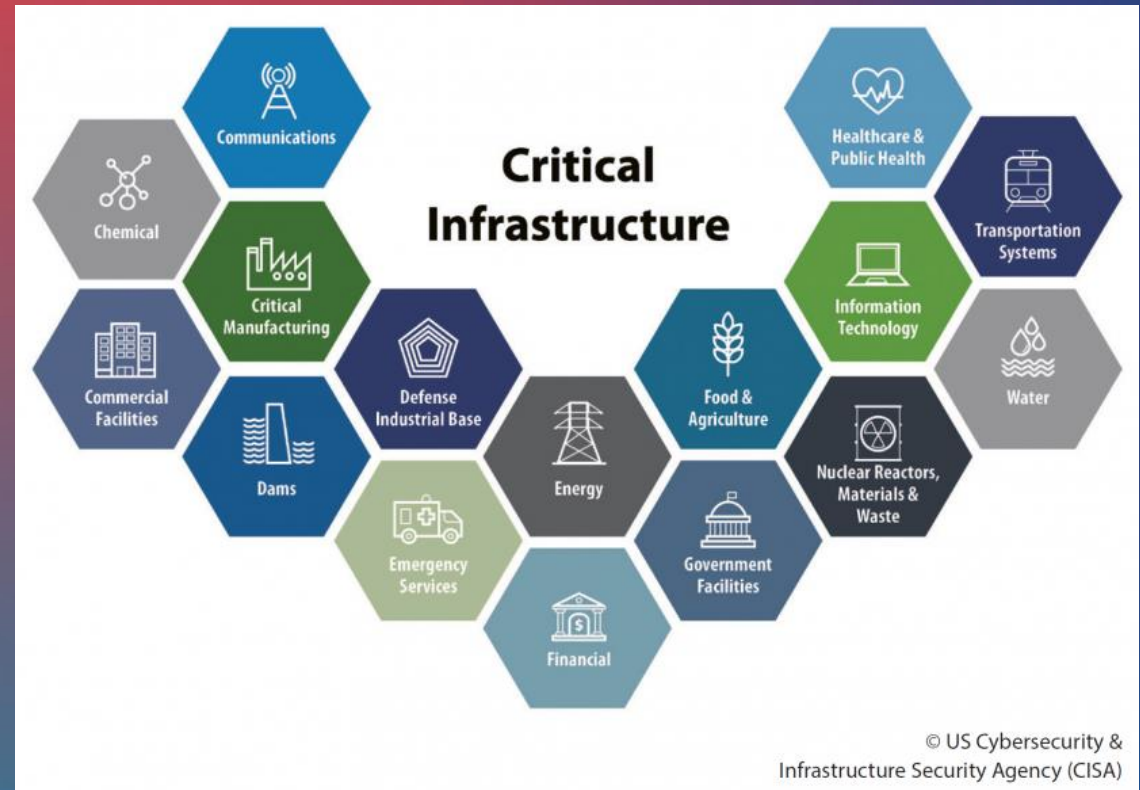
37%
suffered data loss



33%
had to take all systems offline

| | | |
|------------|-----------------------------|------------|
| 25% | EDUCATION | 27% |
| 43% | FINANCE | 34% |
| 40% | HEALTHCARE | 29% |
| 42% | MANUFACTURING/ UTILITIES | 30% |
| 42% | IT/TELECOM | 40% |
| 27% | TRAVEL/ TRANSPORTATION | 24% |

Critical infrastructure and services – such as **healthcare, utilities, communications,** and **transportation** – continue to be **prime targets.**



CHANGE HEALTHCARE CYBERSECURITY INCIDENT





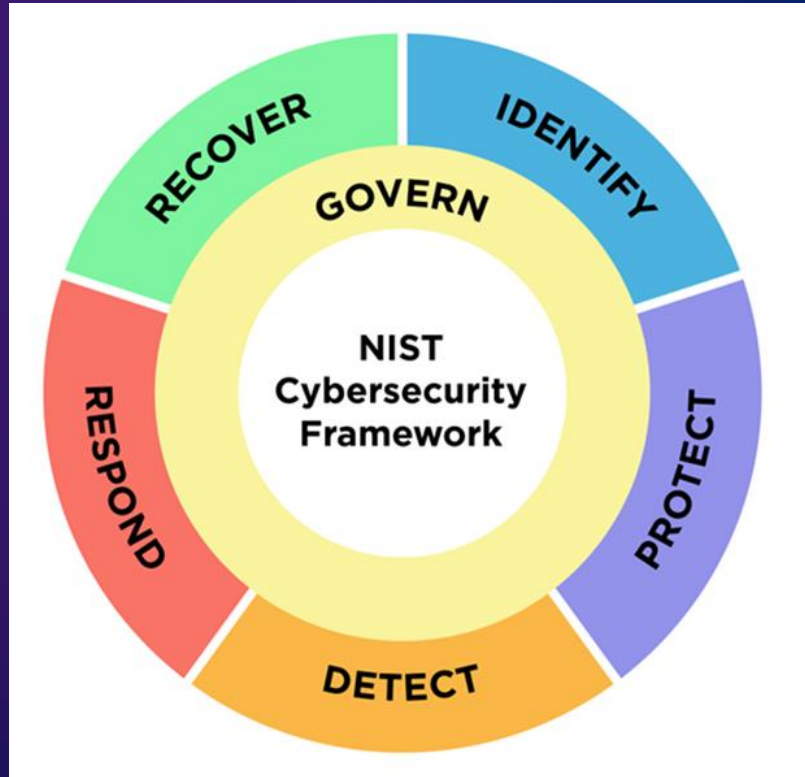
INSURANCE DATA SECURITY- PUERTO RICO REGULATION

Rule No. 108, "Cybersecurity Standards for the Insurance Industry" , based on the NAIC Insurance Data Security Model Law (#668).

OBJECTIVES AND SCOPE

- (1) Protect and ensure the confidentiality, integrity, and availability of insurance industry data;
- (2) Protect data against unauthorized access or use to prevent harm to the consumer;
- (3) Define and periodically reevaluate the data retention period as necessary for operations.

NIST CYBERSECURITY FRAMEWORK



NIST provides a cybersecurity framework (CSF) for best practices to mitigate cybersecurity risks and determine what cybersecurity controls your entity should implement.





NIST CYBERSECURITY FRAMEWORK (CSF) 2.0:

1

Govern: Describes the organizational context, risk management strategy, roles, responsibilities, authority, policies, processes, and oversight.

2

Identify: Describes the categories within each function to manage cybersecurity risk as may be required during operations. Includes identification of assets, risk assessment, impact, and improvements.

3

Protect: Covers controls and processes to ensure authorized availability, integrity, and access to critical infrastructure and services.

4

Detect: Focuses on activities to detect cybersecurity events, either proactively or through alerts and monitoring.

5

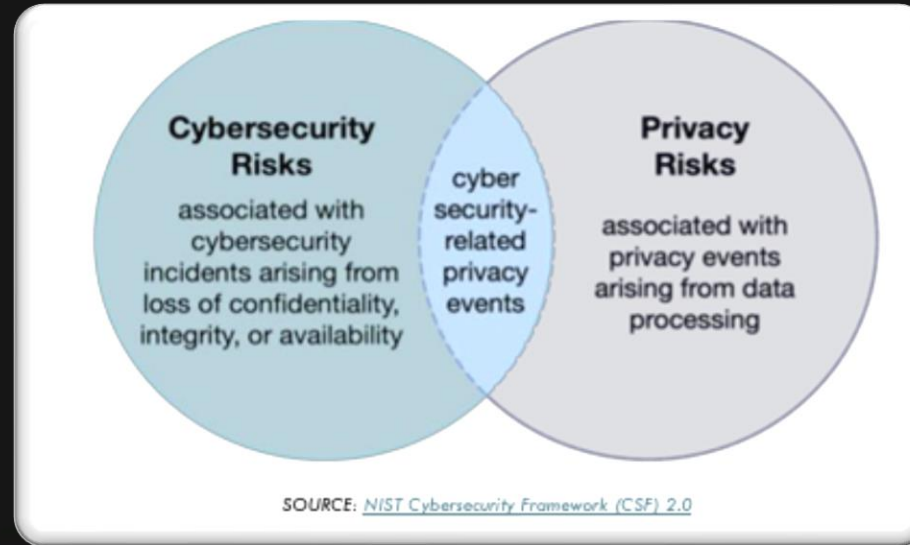
Respond: Defines the actions that will be taken during a cybersecurity incident, from forensic analyses to communications and mitigation.

6

Recover: Restores systems or assets affected by a cybersecurity incident to resume the organization's normal operations.

RELATIONSHIP BETWEEN CYBERSECURITY AND PRIVACY

While cybersecurity and privacy are independent disciplines, their objectives overlap in certain circumstances. A comprehensive cybersecurity program will mitigate privacy risks related to the loss of data confidentiality, integrity, and availability.



GOVERNANCE



ALL STAKEHOLDERS UNDERSTAND AND TAKE INTO CONSIDERATION THE ENTERPRISE'S CYBERSECURITY NEEDS AND EXPECTATIONS.

ROLES, RESPONSIBILITIES, AND AUTHORITIES RELATED TO CYBERSECURITY RISK MANAGEMENT ARE ESTABLISHED, COMMUNICATED, UNDERSTOOD, AND ENFORCED.

Examples:

- An insurer's board of directors should review information technology internal audit findings presenting a material risk to the insurer; and
- Stay informed of emerging cyber threats and vulnerabilities as well as physical threats and conduct periodic cybersecurity training and assessments for their employees and other third parties.

LEGAL, REGULATORY, AND CONTRACTUAL REQUIREMENTS REGARDING CYBERSECURITY – INCLUDING PRIVACY – ARE UNDERSTOOD AND MANAGED.

GOVERNANCE



IMPLEMENT POLICIES AND PROCEDURES TO PROTECT EQUIPMENT, NETWORK, USER ACCOUNTS, AND COMPANY DATA.

Some examples of key policies include:

- Cybersecurity Policy
- Technology Use Policy
- Data Management Policy
- Cybersecurity Employee Training Policy
- Access Control Policy
- Incident Response Policy

IDENTIFICATION



Subscribe at no cost

Cyber Hygiene Services

Cybersecurity and Infrastructure Security Agency

ENROLL

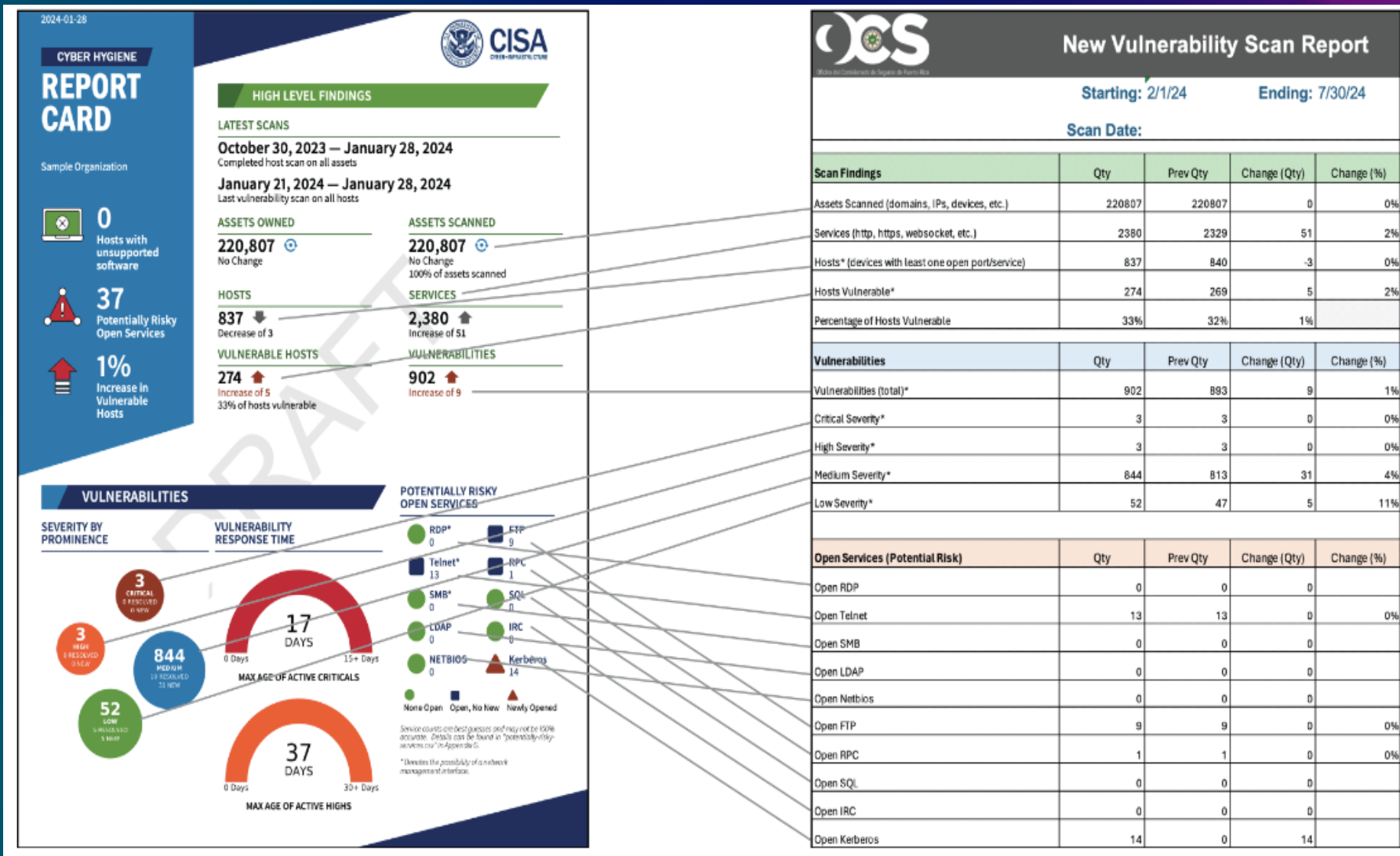
Learn More [▶](#)

Reduce the Risk of a Successful Cyberattack

REGULARLY TEST AND MONITOR SYSTEMS AND PROCEDURES TO DETECT ACTUAL AND ATTEMPTED ATTACKS ON OR INTRUSIONS INTO THE INFORMATION SYSTEM.

PERFORM REGULAR VULNERABILITY TESTS ON THEIR INFORMATION SYSTEMS WITH TOOLS THAT CLEARLY IDENTIFY VULNERABILITIES.

IDENTIFICATION



Each Licensee shall report to the PR-OCS the results of its vulnerability scans twice a year, regardless of the service provider they choose.

Licensees who are enrolled in CISA's Cyber Hygiene Services can easily find the information required to prepare their reports.

IDENTIFICATION

CYBER HYGIENE SERVICES

cisa.gov/CyHyServices



What are the objectives of CISA's Cyber Hygiene Services ?

- **Significantly Reduce Risk-** Organizations typically reduce their risk and exposure by 40%.
- **Avoid Surprises-** Because the services look for assets exposed to the internet; they identify vulnerabilities that could otherwise go unmanaged.
- **Sharpen Your Response-** By combining the vulnerability insights gained with existing threat detection and risk management efforts, enrolled organizations can increase the accuracy and effectiveness of response activities.
- **Broaden Your Security Horizon-** From basic asset awareness to daily alerts on urgent findings, organizations will be in a better place to make risk-informed decisions.

PROTECTION



ESTABLISH EFFECTIVE ACCESS CONTROLS ON INFORMATION SYSTEMS, INCLUDING CONTROLS TO AUTHENTICATE (SUCH AS MULTI-FACTOR AUTHENTICATION) AND ALLOW ACCESS ONLY TO AUTHORIZED INDIVIDUALS

MAINTAIN A FORMAL TRAINING PROGRAM ON CYBER RISK MODALITIES FOR THE STAFF AND KEEP TRACK OF EMPLOYEE PERFORMANCE IN THE PROGRAM.

PROVIDE EMPLOYEES WITH CYBERSECURITY PROGRAM TRAINING AND ASSIGN THEM RESPONSIBILITIES WITHIN THE PROGRAM.

DETECTION



THE DETECT FUNCTION FOCUSES ON FINDING AND ANALYZING POSSIBLE CYBERATTACKS AND THREATS.

INCLUDE BACKUP, SAFEKEEPING, AND MANAGEMENT PROCESSES (“AUDIT LOGS”) WITHIN THE CYBERSECURITY PROGRAM DESIGNED TO DETECT AND RESPOND TO CYBERSECURITY INCIDENTS.

REGULARLY TEST AND MONITOR SYSTEMS AND PROCEDURES TO DETECT ACTUAL AND ATTEMPTED ATTACKS ON OR INTRUSIONS INTO THE INFORMATION SYSTEM AND THE NETWORK



RESPONSE

The incident response plan shall address the following:

| | | |
|---|---|---|
| <p>Description of how the information was exposed, lost, stolen, or breached.</p> | <p>How the cybersecurity event was discovered.</p> | <p>The identity of the source of the cybersecurity event.</p> |
| <p>Description of the specific types of information acquired without authorization.</p> | <p>The period during which the information system was compromised by the cybersecurity event.</p> | <p>The number of total consumers in this state affected by the cybersecurity event.</p> |
| <p>The results of any internal review identifying a lapse in either automated controls or internal procedures or confirming that all automated controls or internal procedures were followed.</p> | <p>Description of efforts being undertaken to remediate the situation which permitted the cybersecurity event to occur.</p> | <p>Communication to government, or law enforcement agencies.</p> |

RECOVERY



THE RECOVER FUNCTION INVOLVES RESTORING ASSETS AND OPERATIONS AFFECTED BY A CYBERSECURITY INCIDENT.

RECOVERY FUCTIONS SHALL ADDRESS:

- IDENTIFICATION OF REQUIREMENTS FOR THE REMEDIATION OF ANY IDENTIFIED WEAKNESSES IN THE INFORMATION SYSTEM.
- DOCUMENTATION AND PREPARATION OF REPORTS REGARDING CYBERSECURITY INCIDENTS AND RELATED RESPONSE ACTIVITIES.
- THE EVALUATION AND REVISION OF THE INCIDENT RESPONSE PLAN, AS NECESSARY.



SUMMARY

RISK ASSESSMENT

Conduct periodic risk assessment to identifying reasonably foreseeable internal and external threats.

THIRD-PARTY SERVICE PROVIDERS

Exercise due diligence when working with third-party service providers and implement measures to protect systems and information.

INFORMATION SECURITY PROGRAM

Maintain a comprehensive written information security program with appropriate physical, technical and administrative controls.

INCIDENT RESPONSE PLAN

Incident response plan outlining how will respond to and recover from a cybersecurity event.

COMMUNICATION

Communication channels established for event notification should provide security for cybersecurity event data-in-transit and data-at-rest.



“

**A breach alone is not a
disaster, but mishandling it is.**



- Serene Davis-

”

THANK YOU!