Ransomware Readiness Statement

What is Ransomware

Ransomware is a sophisticated attack by malware that targets the victim's files and operating system followed by a ransom demand (or demands) to allow the victim to regain access to their data.

Scope and Purpose

The purpose of this document is to outline Ex Libris' readiness against a ransomware attack; to describe the preventive measures Ex Libris has in place in case of an event, or to manage such an event if it were to occur.

Method

Ex Libris has established several different measures in preparation for such an event. The measures include readiness, prevention, identification, containment, assessment, remediation, and monitoring phases, which can be divided into three categories:

- Process
- Technical
- People

Security Measures

Process – Policies, Procedures and Certifications

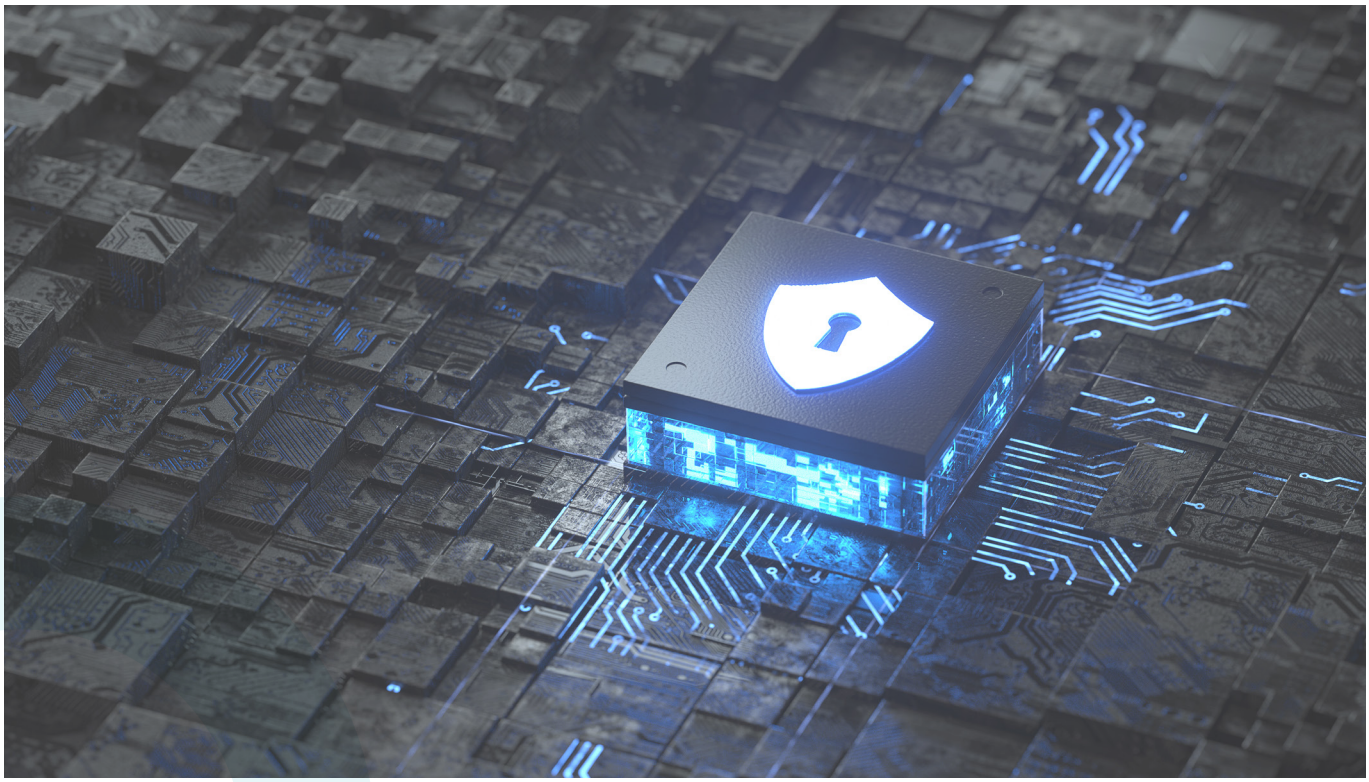
- **ISO 27032 Certification –** A recognized standard that provides guidance on cybersecurity for organizations. The Standard is designed to help organizations protect themselves against cyber-attacks.
- **ISO 22301 Certification –** A comprehensive standard for planning, monitoring, maintaining, documenting, and continually improving a system for business continuity management and disaster preparedness and ransomware testing drills.
- **Cloud Services Business Continuity Planning (BCP) -** Ex Libris maintains a comprehensive Business Continuity Plan for our cloud services. This plan is tested at least annually.
- **Security And Privacy Incident Response Policy -** Ex Libris has implemented an incident response procedure that establishes responsibility and accountability. It defines the steps required to ensure that security incidents are identified, contained, investigated, remedied, communicated, and documented.
- **Patches and Vulnerabilities Assessments Policy -** Ex Libris continually seeks to ensure that its solutions do not contain vulnerabilities that may compromise the security of its products. Ex Libris has implemented a security assessment process for third party software components used with Ex Libris products and security patches and vulnerabilities.
- **Procedures**
  - Ex Libris has a dedicated procedure of Ransomware response.
  - Ex Libris has created a dedicated procedure to isolate a device from the network.
  - Insurance - Ex Libris has insurance in case of a ransomware incident.
  - In case of an incident, Ex Libris engages with technical experts and negotiators from an external security company.
- **Testing**
  - Ex Libris has put in place Readiness testing of plans.
  - Technical and management drills – Ex Libris has defined a scenario involving IT and cloud infrastructure, to test technical skills readiness. Ex Libris tests decisions and checklists in addition to communication approaches, handling media and press releases.
- Continuously auditing - internal audit and independent external audit by external security companies. Processes and penetration testing processes to ensure measures are in place.

Technical measures

- Following security best practices for preventing unauthorized access.
- Disabling unnecessary macros in Office documents that come from the Internet.
- Real-time testing of employees for phishing and other suspicious types of emails.
- Malware protection system that protects against viruses, spyware, and Trojans.
- Enhanced network segregation.
- Ransomware endpoint protection for cloud staff workstations.
- Prohibiting executable attachments and USB mass media usage.
- Ensuring group policies are current; changing default passwords; applying Multi Factor Authentication (MFA) to business systems; enforcing least privileges principles.
- 24/7 HUB - System disruptions are escalated to the HUB immediately.
- Malware protection - Backup and restore measures – protection against blended attacks and destructive attacks, triple extortion attacks (DDoS protection).

Please note

Ransomware readiness is everyone's concern. Users share the responsibilities and must keep their local systems secure.



People – Ransomware Readiness Training

- Education provided to engineers for improving security
- User Awareness training –
  - Phishing simulations,
  - Business Email Compromise (BEC) fraud,
  - Malicious spam (malspam) and by extension ransomware and malware incidents.
  - What to do if contacted (reporting issues)
- Ransomware process and technical training

About Ex Libris

Ex Libris, Part of **Clarivate**, is a leading global provider of cloud-based solutions for higher education. Offering SaaS solutions for the management and discovery of the fullspectrum of library and scholarly materials, as well as mobile campus solutions driving student engagement and success, Ex Libris serves thousands of customers in 90 countries.

Visit www.exlibrisgroup.com

Ex Libris
Part of Clarivate