Ransomware Readiness

Ransomware is a top cyber risk concern for today's businesses. Increased sophistication and frequency of ransomware attacks, coupled with highly-remote workforces that extend the traditional security perimeter, put today's organizations at an increased risk of attack.

Ransomware by the Numbers[1]

4,000

Daily # of ransomware attacks

$233,817

Average ransom

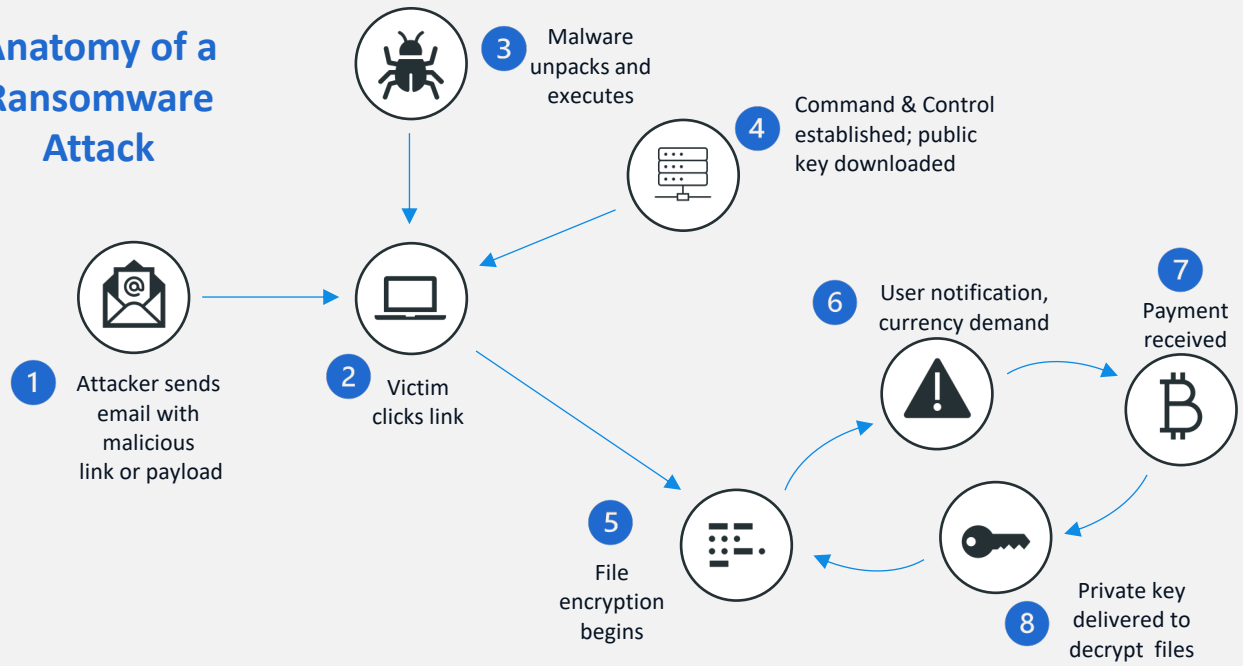
19 days

Average downtime due to an attack

$20B

Expected global ransomware recovery cost in 2021

Anatomy of a Ransomware Attack



A comprehensive, tested, and broadly communicated ransomware readiness plan is the best defense businesses have against an attack.

[1] SafeatLast, 22 Shocking Ransomware Statistics for Cybersecurity in 2021, https://safeatlast.co/blog/ransomware-statistics/#gref

1855 Gateway Blvd. Suite 730, Concord, CA 94520 info@e360.com e360.com

Our Approach to Ransomware Readiness

We offer three levels of assessment to suit organizations with different needs, and across levels of security maturity.

	Rapid Readiness Exercise	Self-Assessment	Full Assessment
Goal	Rapid evaluation of your ransomware readiness plan.	Online self-assessment evaluating key areas that comprise a strong ransomware readiness program.	In-depth ransomware readiness assessment using real world scenarios and industry best practices such as NIST CSF.*
Ideal for	Small to medium sized organizations with limited IT/ security resources.	Medium to large organizations with existing capabilities and knowledge of ransomware.	Medium to large organizations seeking a sophisticated and industry leading ransomware readiness evaluation.
Outcomes	Recommendations to establish a readiness plan against the *Identify, Protect, Detect, Respond,* and *Recover* functions of the NIST CSF* framework.	• Risk rating score. • Ransomware readiness strengths and gaps. • Recommended remediation activities to bolster your plan.	• Risk rating score. • Report of ransomware readiness based on test scenario responses. • Recommended remediation activities.

*NIST CSF: National Institute of Standards and Technology Cybersecurity Framework.

Why Choose e360?

EXPERTISE
We have worked across leading ransomware technologies and can serve as trusted advisors to help you select any necessary technologies to support your readiness plan.

RELEVANT ASSESSMENTS
In addition to the industry leading NIST 1800 frameworks, our assessments are based on real life ransomware scenarios from our previous experience.

EXPERIENCED
Our team comprises senior cyber security professionals with extensive experience detecting, responding and recovering from ransomware attacks.

Contact us to learn more.

1855 Gateway Blvd. Suite 730
Concord, CA 94520
info@e360.com
e360.com

Brad Bussie
Senior Vice President
Security
security@e360.com

Casey Abernethy
Regional Director of Cybersecurity
Security
security@e360.com