Ransomware Risks and Recommendations

"Threat actors continue to pound away at organizations with a variety of new and previously seen ransomware strains, often leaving a trail of destruction in their wake."[1] The U.S. Treasury says ransomware payouts in 2021 could top the entire past decade. Understand today's risks and take action based on FortiGuard recommendations.

Risks and Damages

1100% Increase
The rise of incidents in 2021[2]

$5.2 Billion
The ransom payouts tied to the top 10 hacker groups in 2021[3]

150,000 Detections
The number of individual ransomware detections per week[4]

62% of Organizations
Concerned about losing data due to ransomware[5]

38% of Organizations
Worry about productivity loss[6]

36% of Organizations
Concerned about interruption of operations[7]

9 MONTHS
The time it could take to recover from a ransomware attack[8]

Not to mention the negative financial impacts and reputational damage that ransomware can cause.

The overall frequency of ransomware detections might be leveling off, but the sophistication, aggressiveness, and impact of this threat continues relentlessly.[9]

Actions and Recommendations

By 2024, organizations adopting a **cybersecurity mesh architecture** to integrate security tools to work as a collaborative ecosystem will reduce the financial impact of individual security incidents by an average of **90%.**[10]

Top cybersecurity leaders recommend these 4 critical strategies to address ransomware:[11]

1 Defend:

Starting with access identity management, including MFA, know who and what is on your network. Compartmentalize access and use segmentation to slow and isolate malware. And basic IT hygiene, such as patching, needs to be prioritized.

2 Triage:

Slow the attack, slow the attacker. Limit privilege access to buy critical time, segment the network, and maintain good cyber hygiene.

3 Recovery:

Prevention tactics should also be included in recovery plans, such as quickly pivoting to the cloud to ensure business continuity and creating a "clean room" that replicates infrastructure to ensure faster recovery times.

4 Effective strategies start from the top down:

Company executives, legal, corporate communications, and HR all need to be involved in planning and executing a crisis-management strategy.

[1] "Global Threat Landscape Report: A Semiannual Report by FortiGuard Labs," Fortinet, August 2021.
[2] Ibid.
[3] Mitchell Clark, "US Treasury says ransomware payouts in 2021 could top entire past decade," The Verge, October 15, 2021.
[4] "Global Threat Landscape Report: A Semiannual Report by FortiGuard Labs," Fortinet, August 2021.
[5] "The 2021 Ransomware Survey Report," Fortinet, November 3, 2021.
[6] Ibid.
[7] Ibid.
[8] Mike McGlynn, VP, Global Security Solutions, WWT, Fortinet Security Summit Discusses Practical Insights for Cybersecurity Leaders.
[9] "Global Threat Landscape Report: A Semiannual Report by FortiGuard Labs," Fortinet, August 2021.
[10] "Top Strategic Technology Trends for 2022: Cybersecurity Mesh," Gartner, October 2021.
[11] Fortinet Security Summit Discusses Practical Insights for Cybersecurity Leaders.

Review our ransomware protection checklist to assess your own readiness.

View the PDF