CyberCatch

2022

SMBRS

SMALL AND MEDIUM-SIZED BUSINESSES RANSOMWARE SURVEY

Scope

The SMBRS is a blind survey sponsored by CyberCatch of 1,200 randomly selected small and medium-sized businesses (SMBs) in U.S. and Canada. SMB respondents were less than 500 employee organizations, and included for-profit as well as not-for-profit. Survey respondents were owners, CEOs, senior management or IT management at SMBs. The survey was conducted independently by Momentive, a leading market insights company and maker of SurveyMonkey. The name of the survey sponsor, CyberCatch, was kept confidential in order to prevent any bias in the survey responses.

Survey Focus

The purpose of the survey was to ask SMB respondents a short list of questions to identify susceptibility and resiliency to a ransomware attack.

Ransomware is an existential threat to SMBs, and increasingly SMBs in U.S. and Canada are falling victim. Primarily, attackers either exploit vulnerabilities on Internet-facing IT assets or use phishing emails to break into SMBs networks and install ransomware and encrypt files and systems so they are inaccessible or inoperable, until a ransom is paid.

OVERALL SURVEY RESULTS

30% of SMBs do not have a written incident response plan to respond to threats such as a ransomware attack.

Of those that have a plan... **35%** tested the plan over six months ago.

21% do not have backups offline that cannot be encrypted by ransomware.

34% do not test employees for susceptibility to phishing.

75% would **survive only 3 to 7 days from a ransomware attack.**

47% would survive only **3 DAYS** from a ransomware attack.

28% would survive only **7 DAYS** from a ransomware attack.

Key Findings by SMB Types

LIFE SCIENCE COMPANIES

50% of life science companies **do not have** a written incident response plan.

Of those that have a plan... **100%** tested the plan over six months ago.

83% would **survive only 3 to 7 days** from a ransomware attack

LAW FIRMS

50% of law firms **do not have** a written incident response plan.

Of those that have a plan... **36%** tested the plan over six months ago.

83% would **survive only 3 to 7 days** from a ransomware attack

PROFESSIONAL SERVICES

45% of professional service providers **do not have** a written incident response plan.

Of those that have a plan... **35%** tested the plan over six months ago.

67% would **survive only 3 to 7 days** from a ransomware attack

INSURANCE BROKERS

42% of insurance brokers **do not have** a written incident response plan.

Of those that have a plan... **64%** tested the plan over six months ago.

84% would **survive only 3 to 7 days** from a ransomware attack

NON-PROFIT ORGANIZATIONS

37% of non-profits **do not have** a written incident response plan.

Of those that have a plan... **65%** tested the plan over six months ago.

72% would **survive only 3 to 7 days** from a ransomware attack

RETAIL

37% of retail companies **do not have** a written incident response plan.

Of those that have a plan... **35%** tested the plan over six months ago.

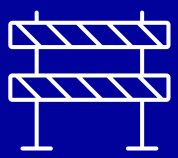
70% would **survive only 3 to 7 days** from a ransomware attack

Survey Results Details by SMB Type

ACCOUNTING FIRMS

- 14% have no written Incident Response Plan
- Of those with a plan, 29% tested the plan over 6 months ago
- 31% have no backups offline
- 27% don't perform phishing testing of employees
- 48% would survive only 3 days from a ransomware attack
- 23% would survive only 7 days from a ransomware attack
- 29% would survive more than 7 days from a ransomware attack

CONSTRUCTION COMPANIES



- 36% have no written Incident Response Plan
- Of those with a plan, 24% tested the plan over 6 months ago
- 20% have no backups offline
- 39% don't perform phishing testing of employees
- 47% would survive only 3 days from a ransomware attack
- 23% would survive only 7 days from a ransomware attack
- 30% would survive more than 7 days from a ransomware attack

EDUCATION

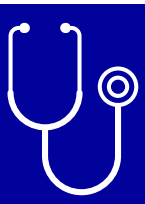
- 26% have no written Incident Response Plan
- Of those with a plan, 50% tested the plan over 6 months ago
- 21% have no backups offline
- 34% don't perform phishing testing of employees
- 34% would survive only 3 days from a ransomware attack
- 37% would survive only 7 days from a ransomware attack
- 29% would survive more than 7 days from a ransomware attack

FEDERAL GOVERNMENT

- 9% have no written Incident Response Plan
- Of those with a plan, 25% tested the plan over 6 months ago
- 22% have no backups offline
- 18% don't perform phishing testing of employees
- 64% would survive only 3 days from a ransomware attack
- 18% would survive only 7 days from a ransomware attack
- 18% would survive more than 7 days from a ransomware attack

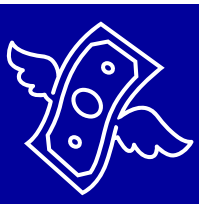
Survey Results Details by SMB Type (cont.)

HEALTHCARE



- 21% have no written Incident Response Plan
- Of those with a plan, 42% tested the plan over 6 months ago
- 8% have no backups offline
- 30% don't perform phishing testing of employees
- 59% would survive only 3 days from a ransomware attack
- 24% would survive only 7 days from a ransomware attack
- 17% would survive more than 7 days from a ransomware attack

INSURANCE PROVIDERS



- 42% have no written Incident Response Plan
- Of those with a plan, 64% tested the plan over 6 months ago
- 18% have no backups offline
- 32% don't perform phishing testing of employees
- 42% would survive only 3 days from a ransomware attack
- 42% would survive only 7 days from a ransomware attack
- 16% would survive more than 7 days from a ransomware attack

LAW FIRMS

- 50% have no written Incident Response Plan
- Of those with a plan, 37% tested the plan over 6 months ago
- 23% have no backups offline
- 58% don't perform phishing testing of employees
- 53% would survive only 3 days from a ransomware attack
- 30% would survive only 7 days from a ransomware attack
- 17% would survive more than 7 days from a ransomware attack

LIFE SCIENCES

- 50% have no written Incident Response Plan
- Of those with a plan, 100% tested the plan over 6 months ago
- 17% have no backups offline
- 67% don't perform phishing testing of employees
- 33% would survive only 3 days from a ransomware attack
- 50% would survive only 7 days from a ransomware attack
- 17% would survive more than 7 days from a ransomware attack

Survey Results Details by SMB Type (cont.)

LOCAL GOVERNMENT

- 21% have no written Incident Response Plan
- Of those with a plan, 40% tested the plan over 6 months ago
- 19% have no backups offline
- 36% don't perform phishing testing of employees
- 61% would survive only 3 days from a ransomware attack
- 11% would survive only 7 days from a ransomware attack
- 28% would survive more than 7 days from a ransomware attack

MANUFACTURERS

- 27% have no written Incident Response Plan
- Of those with a plan, 31% tested the plan over 6 months ago
- 17% have no backups offline
- 31% don't perform phishing testing of employees
- 48% would survive only 3 days from a ransomware attack
- 26% would survive only 7 days from a ransomware attack
- 26% would survive more than 7 days from a ransomware attack

NON-PROFIT ORGANIZATIONS

- 37% have no written Incident Response Plan
- Of those with a plan, 65% tested the plan over 6 months ago
- 28% have no backups offline
- 47% don't perform phishing testing of employees
- 37% would survive only 3 days from a ransomware attack
- 35% would survive only 7 days from a ransomware attack
- 28% would survive more than 7 days from a ransomware attack

PROFESSIONAL SERVICES

- 45% have no written Incident Response Plan
- Of those with a plan, 35% tested the plan over 6 months ago
- 23% have no backups offline
- 39% don't perform phishing testing of employees
- 41% would survive only 3 days from a ransomware attack
- 26% would survive only 7 days from a ransomware attack
- 33% would survive more than 7 days from a ransomware attack

Survey Results Details by SMB Type (cont.)

RETAIL

- 37% have no written Incident Response Plan
- Of those with a plan, 35% tested the plan over 6 months ago
- 17% have no backups offline
- 42% don't perform phishing testing of employees
- 42% would survive only 3 days from a ransomware attack
- 28% would survive only 7 days from a ransomware attack
- 30% would survive more than 7 days from a ransomware attack

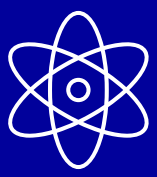
TECHNOLOGY MANUFACTURERS

- 15% have no written Incident Response Plan
- Of those with a plan, 34% tested the plan over 6 months ago
- 15% have no backups offline
- 16% don't perform phishing testing of employees
- 45% would survive only 3 days from a ransomware attack
- 43% would survive only 7 days from a ransomware attack
- 12% would survive more than 7 days from a ransomware attack

TRANSPORTATION

- 36% have no written Incident Response Plan
- Of those with a plan, 21% tested the plan over 6 months ago
- 32% have no backups offline
- 44% don't perform phishing testing of employees
- 53% would survive only 3 days from a ransomware attack
- 22% would survive only 7 days from a ransomware attack
- 25% would survive more than 7 days from a ransomware attack

UTILITIES & ENERGY



- 8% have no written Incident Response Plan
- Of those with a plan, 63% tested the plan over 6 months ago
- 36% have no backups offline
- 42 % don't perform phishing testing of employees
- 58% would survive only 3 days from a ransomware attack
- 25% would survive only 7 days from a ransomware attack
- 17% would survive more than 7 days from a ransomware attack

Seven Cybersecurity Controls to Thwart Ransomware

1. **Implement a written Incident Response Plan** and test it for ransomware attack at least every six months because threats evolve rapidly.

2. **Regularly scan Internet-facing IT assets for vulnerabilities** and promptly fix so attackers cannot exploit.

3. **Test employees regularly for susceptibility to phishing and social engineering** so they do not inadvertently download ransomware or provide access to attackers for eventual installation.

4. **Segment network and air gap critical IT assets**, so ransomware cannot spread easily.

5. **Require multi-factor authentication (MFA) on all users,** minimally on privileged users, because attackers will steal credentials to install ransomware.

6. **Store backups offline,** otherwise ransomware will find the backups and encrypt.

7. **Continuously test cybersecurity controls from the outside and inside** to find missing or broken controls and fix before attackers can exploit.

CyberCatch

About CyberCatch

CyberCatch is a unique cybersecurity Software-as-a-Service (SaaS) company that protects small and medium-sized businesses (SMBs) from cyberattacks by focusing on the root cause why SMBs fall victim: security holes. CyberCatch provides an innovative cloud-based SaaS platform coupled with deep subject matter expertise to help SMBs implement just the right type and amount of cybersecurity controls. The platform then performs automated testing of controls from three dimensions: outside-in, inside-out and social engineering. It generates the Cyber Breach Score to continuously measure cyber risk, and finds security holes and guides the SMB to fix them promptly, so attackers can't exploit any missing or broken controls to break in and steal data or infect ransomware. CyberCatch's continuous value proposition: Test. Fix. Secure.

For more information:

VISIT WEBSITE