2021 Was the Year of Ransomware: What Can We Expect for 2022?

MICHAEL OSTERMAN
Principal Analyst
Osterman Research, Inc.

OSTERMAN RESEARCH
delivering insight

About Osterman Research

Focused on the messaging, Web and collaboration industries.

Practice areas include archiving, security, encryption, content management, etc.

Strong emphasis on primary research conducted with decision makers and influencers.

Founded in 2001.

Based near Bellevue, Washington and Christchurch, New Zealand.

An Overview

- From 2019 to 2020
  - Malware increased by 358%
  - Ransomware increased by 435%
  - At least 2,354 entities in the US were hit with ransomware
  - >1,300 companies worldwide lost data
  - Key targets were government, healthcare and education

- From 2020 to 2021
  - 93% increase in ransomware in the first half of 2021 compared to the same period in 2020
  - Global cyber attacks are up 29%, most notably in EMEA and the Americas

Data sources: Deep Instinct, Emsisoft and Check Point

Ransomware Incidents That Have Occurred

34% detected ransomware before it was activated

14% suffered a ransomware infection because of phishing

10% resulted in internal IT systems becoming non-operational

6% suffered unrecoverable data loss

6% had a department or business unit cease operations, at least temporarily

4% resulted in OT systems becoming non-operational

3% had to cease operations across the entire organization, at least temporarily

2% saw data exfiltrated as part of a ransomware attack

1% had data exfiltrated and offered for public sale or auction

Data source: Osterman Research

Major Ransomware Incidents in 2021

- JBS Foods: ransom of $11 million was paid
- Colonial Pipeline: 8,850km of pipeline were shut down, resulting in gasoline shortages and public safety risks
- Westrock: caused an 85,000-ton shortfall in production of paper and packaging products within 10 days
- AXA: bad actors stole three terabytes of data
- Brenntag: attackers stole 150 gigabytes of data
- Acer: leaked sensitive corporate content, bad actors demanded $50 million in ransom
- Quanta: attack on this Apple resulted in a leak of sensitive Apple documents
- NBA: bad actors stole 500 gigabytes of confidential information
- CNA: 15,000 devices were encrypted, including those of remote employees
- Kaseya: bad actors used a bogus software update to infect one million systems
- Irish Dept. of Health and the Health Service Executive: significant cancellations in various services

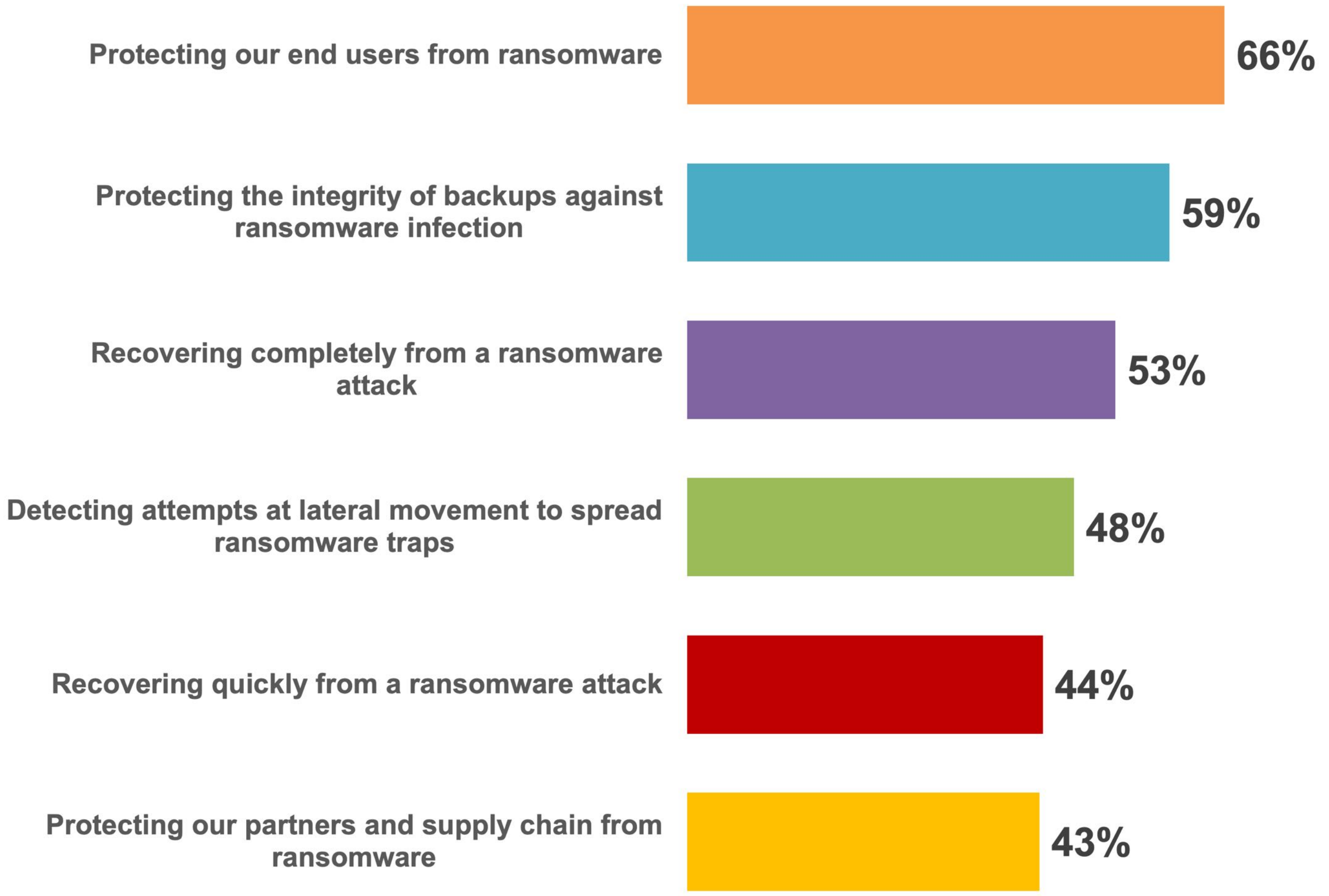
Data source: Various

Organizational Effectiveness on Various Security Problems

% that perceive their organizations as "effective" or "highly effective"

Two-thirds of organizations believe they are effective or highly effective at protecting their end users from ransomware.

Far fewer are this confident about protecting partners and their supply chain, or recovering quickly from an attack.

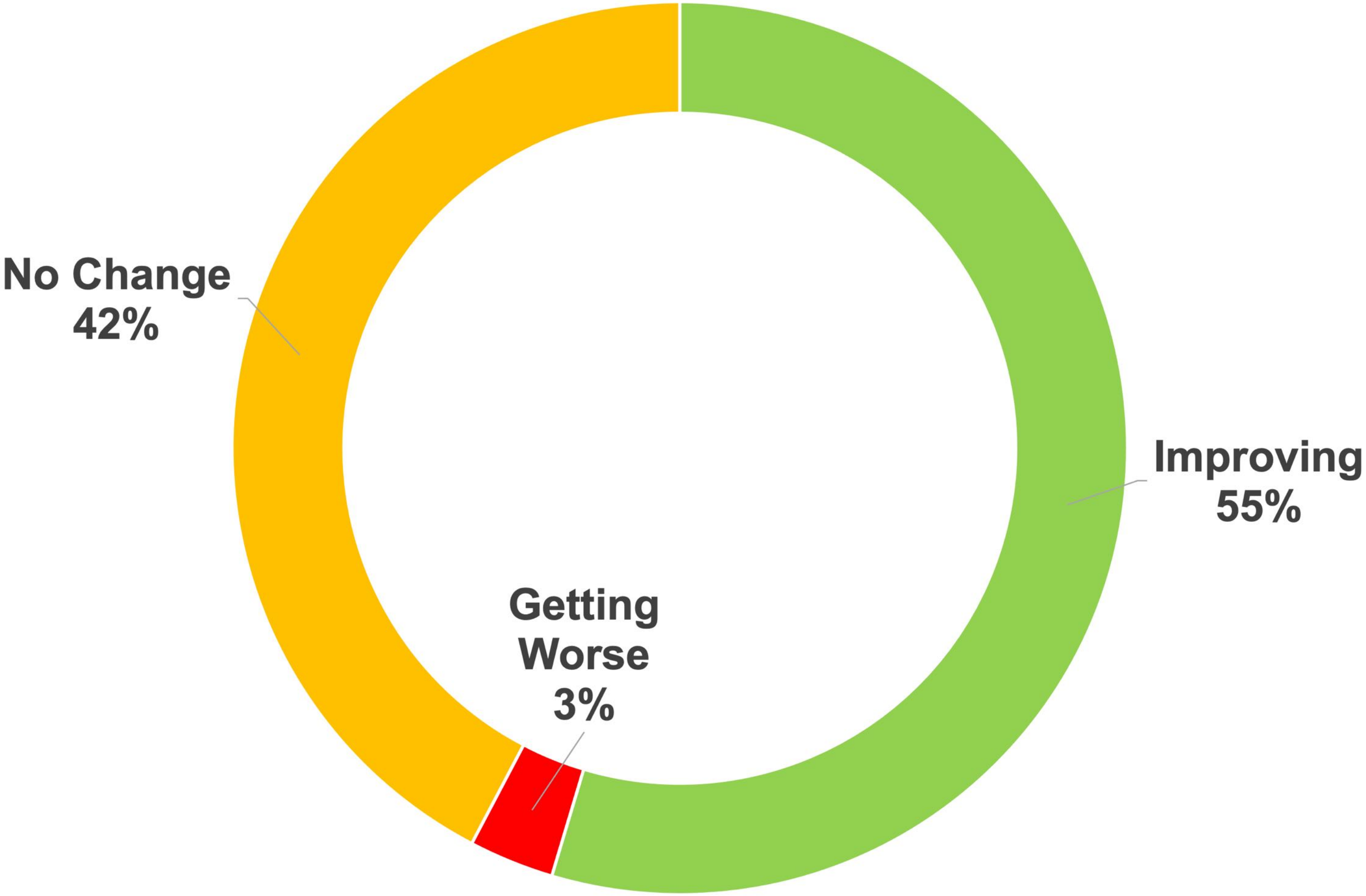


Data source: Osterman Research

Long-Term Changes in Dealing with Ransomware

More than one-half of organizations feel their ability to deal with ransomware infections on their network are improving.

But nearly one-half do not.



Data source: Osterman Research

The Next Wave of Ransomware

- IT has been the traditional target of ransomware criminals

- OT is an increasingly attractive target

- Examples:
  - January 2021: major electric companies Electrobras and Copel in Brazil were impacted by ransomware
  - March 2021: a water system in Nevada was targeted with ransomware that affected SCADA and backup systems
  - July 2021: a wastewater SCADA computer in a facility in Maine was infected with ransomware
  - August 2021: ransomware was deployed in a water system in California one month after the initial breach
  - November 2021: the IT network of CS Energy in Queensland were shut down

Data source: Various

The Target is Enormous

- Public water systems
- Wastewater treatment plants
- Nuclear power plants
- Electrical distribution facilities
- Chemical plants
- Emergency services
- Food processing plants
- Hospitals and other healthcare facilities
- Dams
- Communications systems
- Transportation systems

Two Predictions for 2022

- A big increase in IT-focused attacks, but a larger increase on attacks of OT infrastructure
  - Water treatment plants
  - Electrical grids
  - Communication systems

- An increase in attacks on healthcare facilities
  - Through late May 2021, there were 82 ransomware incidents worldwide against the healthcare sector; health/medical clinics were the primary target*
  - Healthcare records are valuable: $50+ on the black market
  - Healthcare organizations have a large footprint: hospitals, clinics, doctors' offices, healthcare administrators, insurance carriers, and others

* Data source: HHS Cybersecurity Program

Three Areas That Should/Will be Addressed in 2022

- Backups are inadequate – they need to improve
  - Only 59% of organizations surveyed by Osterman Research consider the integrity of their backups against ransomware infection to be “effective” or “highly effective”.
  - Many organizations either do not have adequate backups, or do not have backup that are protected against encryption.
  - The best way to protect backups is to encrypt them and write them to WORM media.

- Training is inadequate – it needs to be improved
  - Phishing is still a reliable method for delivering ransomware.
  - Organizations will be more focused on good security awareness training.

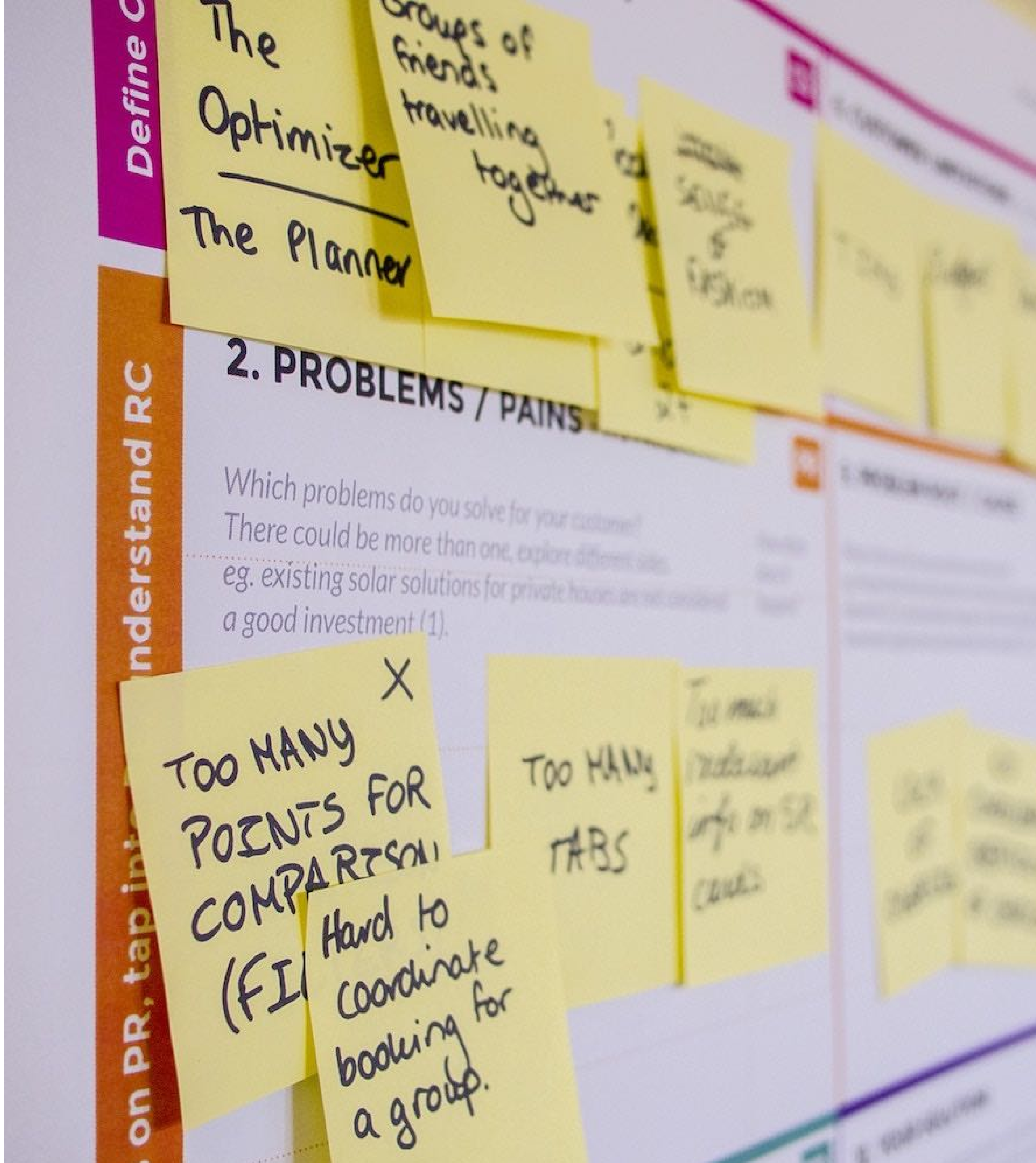
- Multi-factor authentication will be forced on users
  - Only 18% of Microsoft customers use MFA

Summary

Ransomware attacks are becoming increasingly pervasive and expensive.

OT and healthcare will become increasingly attractive targets for bad actors in 2022.

Organizations will respond by making improvements to their backup, training and MFA practices.


Define C
The Optimizer
The Planner
Groups of friends travelling together
2. PROBLEMS / PAINS
Which problems do you solve for your customer?
There could be more than one, explore different sides
eg. existing solar solutions for private houses are not considered
a good investment (1).
Understand RC
on PR, tap into
X
TOO MANY POINTS FOR COMPARISON (FI
TOO MANY TABS
Hard to coordinate booking for a group.

OSTERMAN RESEARCH

delivering insight

Osterman Research, Inc. / Osterman Research Limited

☎ +1 206 683 5683 (US) / +64 21 642 998 (NZ)

info@ostermanresearch.com

www.ostermanresearch.com

@OstermanRsch