House Keeping

1. *All questions can be entered into the Q&A section of Zoom. (Toolbar Tab: Q&A)*

2. *We have a live Poll that can be taken at any time during the webinar. (Toolbar Tab: Poll)*

3. *Private message Kyle with any concerns, requests, or anonymous questions.*

4. *Our next event will highlight data-privacy and compliance framework, now live on our website!*

Choosing the Right Framework for Your Business - April 26th, 2022 @10:30 AM

Sign Up Now: clarecomputer.com/events

CLARE COMPUTER™
SOLUTIONS
Empower Your Business Success

OMNISTRUCT
CYBERSECURITY PROGRAMS THAT WORK

Introduction

OMNISTRUCT
CYBERSECURITY PROGRAMS THAT WORK

Matt Monroe
Operations Manager
Omnistruct

Matt Oldham
Senior Sales Engineer
Omnistruct

CLARE COMPUTER™
SOLUTIONS
Empower Your Business Success

Rod Sweet
Security Architect
Clare Computer Solutions

Top Threat to SMBs in 2021

1. Ransomware

Ransomware is a form of malicious software that threatens you with harm, usually by denying you access to your data. Ransomware attacks are often deployed via social engineering tactics.

59% said remote work due to COVID-19 resulted in increased ransomware attacks.

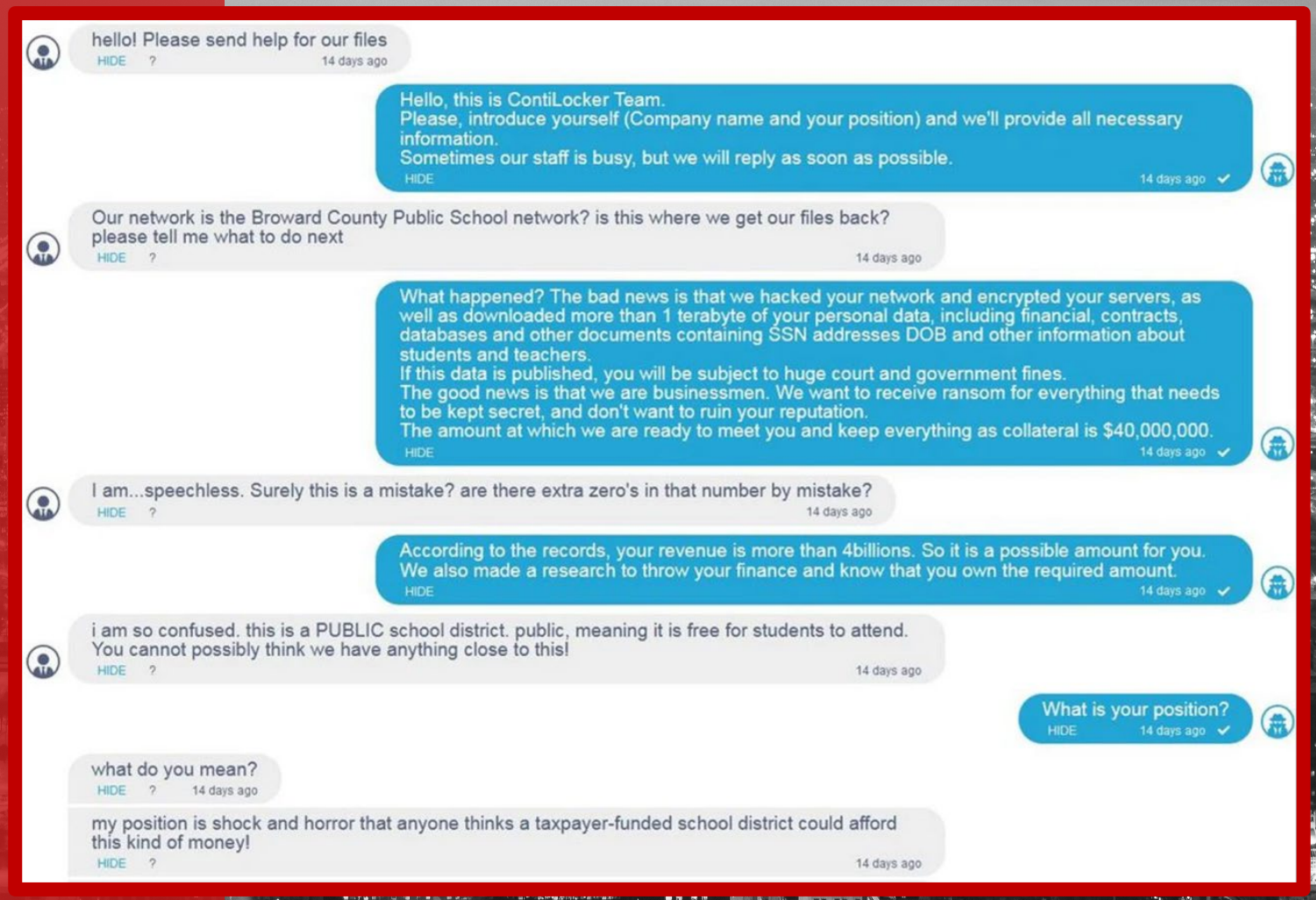
52% reported that shifting client workloads to the cloud came with increased security vulnerabilities.

Broward County Public School Attack

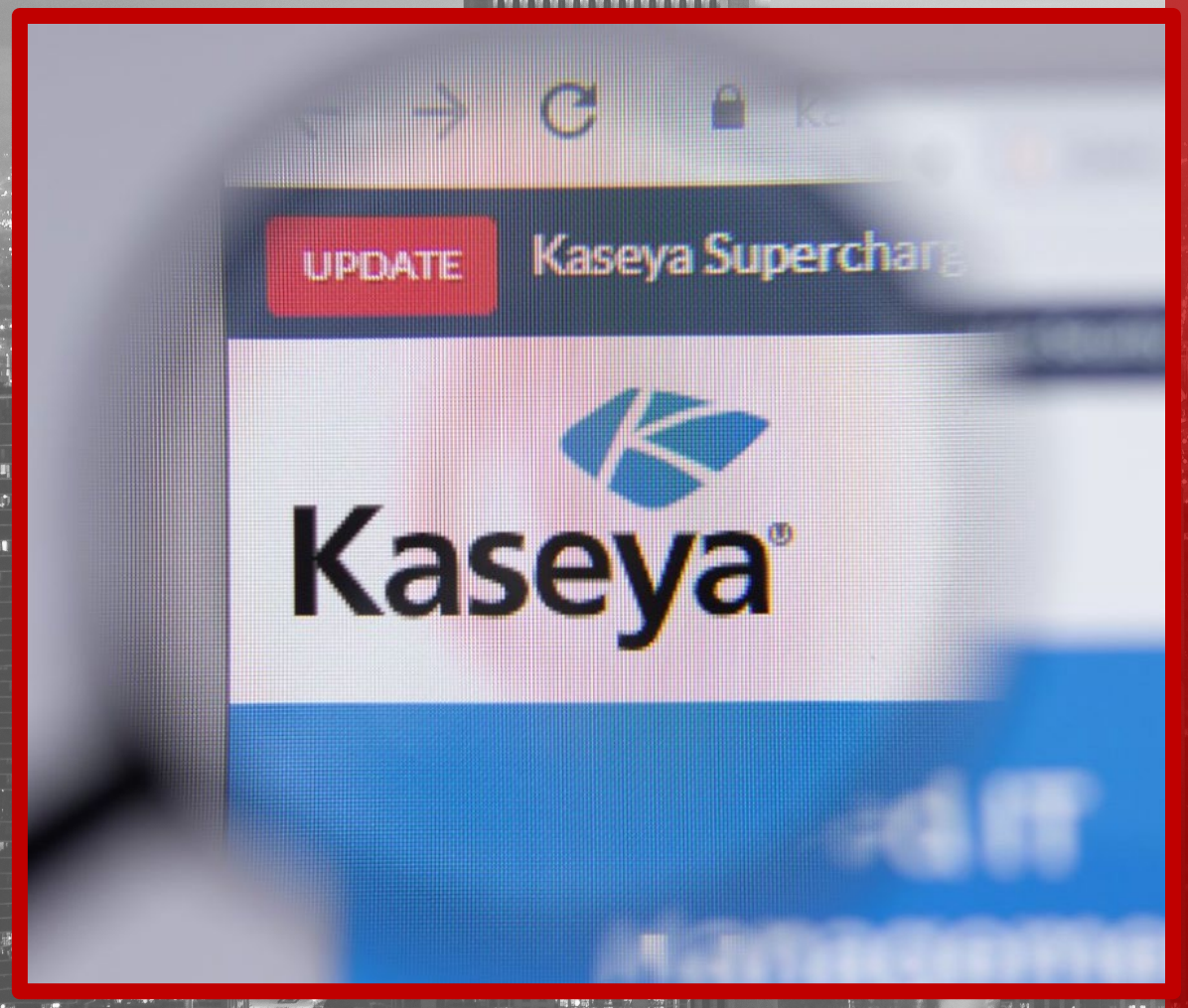
Roughly 50,000 personal records were stolen from employees, students and parents.

Tangible Next Steps:

1. Security Awareness Training (SAT)
2. Backup & Endpoint Security



Kaseya Ransomware Attack



Attackers have carried out a supply chain ransomware attack by leveraging a vulnerability in Kaseya software to steal information of 800 to 1500 Small to medium-sized companies through ransomware

Tangible Next Steps:

1. Least Privilege / Limited Access
2. Patching & Vulnerability Monitoring

Threat Trends for 2022

1. ***Ransomware Continues to top the list - spiking 935% in 2021!***
   - Group-IB's Hi-Tech Crime Trends reports for 2021/2022 stated that an "unholy alliance" between ransomware operators and corporate-access brokers have **fueled a 935% spike** in stolen data.
   - First three quarters of 2021 saw **47% more stolen company data** than in all of 2020
   - Affiliate markets for phishing scams are expanding. Researchers found **70 new phishing-based programs** that allowed the attackers to steal ~$10M last year.

Threat Trends for 2022

2. **Software/Hardware Vulnerabilities and physical devices grew 200% in 2021!**
   - As software gets more secure, hackers are going **deeper into areas of higher privilege**, like the firmware and hardware.
   - The number of connected IoT devices is **expected to grow up to 27 billion** during 2022-2026 with the advent of new technologies for smart homes, wearable devices, and more efficient cars operating with real-time information.
   - Hackers can also mount an attack at the supply chain level and by **exploiting gaps in the security** processes, hackers can inject malicious code into device updates.

Threat Trends for 2022

3. **2022 is shaping up to be a banner year for cybercriminals with attackers lining up to find a victim.**

   - Social Engineering continues rising. Between October and January, COVID test-related **phishing attacks surged 521%**.
   - Cloud threats continue to exploit security practices and configurations **creating many security gaps** from deployment.
   - Log4j was used by the **top 32 technology** companies including, Sophos, Oracle, F-Secure, McAfee, and Amazon!

Additional Tangible Next Steps to Consider

- Ensuring users have strong passwords, enabling MFA wherever possible.
- Security awareness training is the largest target
- Payloads can be downloaded by visiting types of websites
- End-Point Security isn't a first line of defense, it's your last line…
- Incident response plans provide better preparation, in the case of cyber attacks

Ask Yourself:

What's the big picture?

Zoom Out

How do you define best practices to be better prepared and reduce your risk?

Do you follow a set standard or is it a more subjective approach?

- *Importance of being proactive vs reactive*
- *Need for written policies and procedures*

Considerations When Choosing a Framework

1. **Is there a required standard or framework for your industry?**
2. **Are there standards or frameworks that are required to do business with your existing customers and/or target markets?**

Next Event :

Choosing the Right Framework for Your Business – April 26th @10:30AM

Join our high-level review of data privacy and compliance requirements based on your industry, customer data, and location.

More Details: clarecomputer.com/events/

Feel Like You're Drinking From a Fire Hose?

- Like with any new year resolution, the key is getting started
  - *There are some simple things you can do right away to reduce your risk (security awareness training, strong passwords, patching)*
- Start considering a framework to begin the process of maturing your approach to cyber security

Questions & Answers