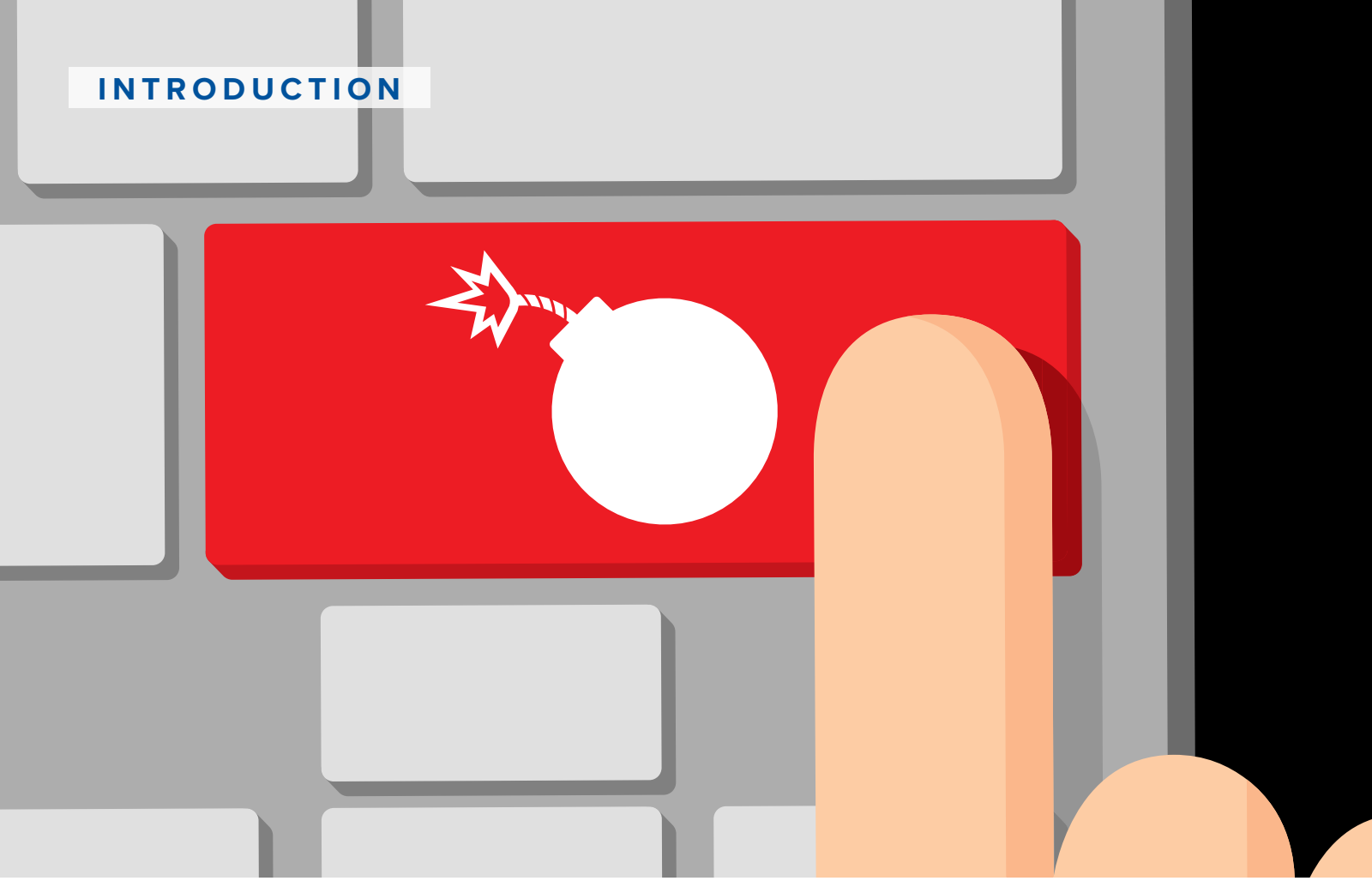
Quantum

SECURING YOUR DATA

with a Multi-Layer Approach to Ransomware Protection and Recovery

INTRODUCTION



Ransomware has proliferated through every vertical and industry and continues its upward trajectory trend. It is costing organizations billions of dollars every year and is expected to exceed $265 billion by 2031. While over two-thirds of organizations worldwide report being affected by ransomware attacks, the most targeted industries are retail, healthcare, and public sector such as governmental bodies or education. In many cases, the attacks render them incapable of offering their critical services to patients and clients, and this affects all of us. Health IT Security reports, **"On average the ransomware attacks cause about 15 days of EHR (Electronic health record) downtime."** Some incidents last more than a month, such as the attacks at University of Vermont Health Network and Universal Health Services (UHS). **"UHS attack impacted all 400 of its US care sites and caused three weeks of downtime, with a total of $67 million in recovery efforts and lost revenue."** At UVM, the attack that occurred cost around $1.5 million per day in lost revenue and expenses to restore its computer systems. When a software supplier to the National Health Service in the UK was the target of an attack, this severely affected services including patient referrals, ambulance dispatch, out-of-hours appointment bookings, mental health services, and emergency prescriptions. And one of the most publicized attacks in recent years brought down the Colonial Pipeline, America's largest "refined products" pipeline. As a result, the average price of a gallon of gas in the US increased to more than $3 for the first time in seven years.

Lack of Security Measures Allows Criminals Access to Your Data

It is not just the security of the network, but of all possible entrances, such as through edge application, IoT, phishing, and of course network front doors and open back doors. Lack of security measures by many companies have allowed this criminal activity to further gain inroads in their insidious attacks to gain access to your most important asset.

Formulating a Strategy to Combat Ransomware

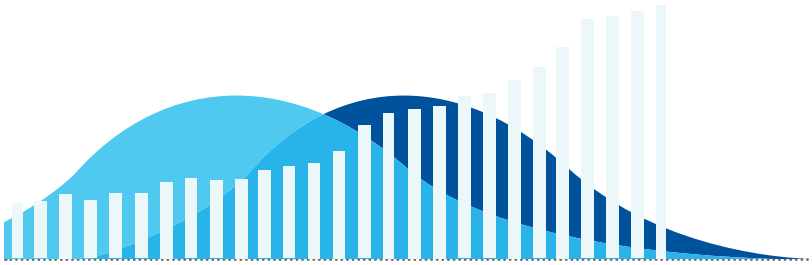
Organizations must be proactive with a solid data protection plan. Relying on an existing backup infrastructure to do the job is no longer enough. A backup and recovery plan evolves over time and it needs to be updated as the threatening environment changes and your technology is refreshed.

Be Proactive in Your Security Approach

As backup is fast becoming the primary target, establishing security measures that protect your backup infrastructure becomes a critical component to address. A multi-layer security approach to ransomware protection and recovery is one of the most cost-effective methods to iron clad your data while keeping costs down. A quote from Sun Tzu in the Art of War that seems to be very applicable in our current state in defending against ransomware: "If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle." Let's not succumb in battle. Instead, be proactive in your security approach.

IT professionals must be proactive in how they approach cybersecurity and evaluate the defense mechanisms by layers.

10 GUIDELINES TO BEING PREPARED FOR A RANSOMWARE ATTACK



1. **Develop a well-conceived data protection strategy to present to management and gain their support. You can't get far without it.**

2. **Reach out to your preferred vendor for help in developing a plan that shows the value of the proposition and how it can mark a differentiation for the broader business.**

3. **Implement anti-virus software to close the front door entrance to the network.**

4. **Leverage encryption technology in all stages of the data: at rest, in transit, and active.**

5. **Provide your employees with security training and educate them on the main methods used by criminals to gain access into networks and systems, especially phishing methods.**

6. **Implement immutable capabilities that create snapshots of your data and allow for immediate recovery to meet or exceed your SLAs' RPO/RTO needs.**

7. **Deploy solutions such as tape storage, that have air-gapping capabilities to protect data indefinitely for long-term protection.**

8. **Replicate data offsite. You may also leverage a cloud or object storage solution for disaster recovery.**

9. **Implement network segmentation to limit the spread of an attack. It is one of the best mitigations against data breaches, ransomware, and other malware infections.**

10. **Cyber insurance is a must, but employ it only as a last resort.**

BEING PREPARED IS ONLY PART OF THE EQUATION

Attackers are targeting your backup infrastructure.

Let's look at a few simple ways to secure your data platforms and implement a solid backup strategy...

6 STEPS TO CHOOSING SECURE DATA PLATFORMS AND IMPLEMENTING A BACKUP STRATEGY

Security needs to be a key consideration when selecting data storage platforms. If you are leveraging the public cloud, or your workloads are spread across multiple clouds and compute environments, you will need additional privacy and security controls beyond those in your own network. You need a comprehensive approach that will require multiple departments, including security professionals, network administrators, and their leaders. Take the reasonable steps to educate yourself and your users, especially with a remote workforce.

1 Identify where vulnerabilities might exist.

2 Implement reputable anti-virus software—this should be non-negotiable.

3 Conduct frequent backups. Adhere to the 3-2-1-1 best practice backup rule to ensure you have the safety protocols in place in case of any disaster including ransomware.

4 Consider behavior analysis technologies that can detect anomalies at endpoints.

5 Keep offline copies (as recommended by the FBI, CISA, and NCSC UK).

6 Determine whether disk, tape (onsite or cold storage in cloud), or cloud/object storage will be the best recovery method for your organization – Consider your SLAs.

RANSOMWARE PROTECTION MUST COME IN LAYERS

We all need to work together to protect the cyber climate for the next five to ten years. We need to empower enterprises and SMBs to implement solid proactive strategies and guidelines that can be cost-effective. As those methods evolve, we need to employ technologies, such as machine learning (ML) and artificial intelligence (AI), to provide the advanced security analytics needed to stay ahead of the criminals. But of course, mitigating risk takes multiple technologies. Not one single solution can achieve the protection you will need for the assault organizations are experiencing. Ransomware protection must come in layers. Bringing this dark market to a halt also requires changes in processes, technologies, backup methodologies, and attitudes. Investing in training will also be key. And because these attacks are no longer isolated incidents, we can no longer work in isolation. We must document and share knowledge about our unfortunate ransomware experiences so we can begin the work to recover from this cyber crisis.

A multi-layer approach to ransomware protection and recovery is the most cost-effective method to implement a ransomware recovery strategy by moving data to different tiers depending on your needs and your data's lifecycle. Quantum is the data protection expert; our solutions are unique because we help you keep costs down while ensuring your data is fully secured in isolation or behind a physical air-gap barrier that keeps data immutable. Ransomware cannot infiltrate what it can't reach.

Mitigating risk takes multiple technologies. Ransomware protection must come in layers.

To learn more about Quantum's ransomware recovery solutions, visit: **www.quantum.com/ransomware-recovery**

Quantum®

ABOUT QUANTUM

Quantum technology, software, and services provide the solutions that today's organizations need to make video and other unstructured data smarter – so their data works for them and not the other way around. With over 40 years of innovation, Quantum's end-to-end platform is uniquely equipped to orchestrate, protect, and enrich data across its lifecycle, providing enhanced intelligence and actionable insights. Leading organizations in cloud services, entertainment, government, research, education, transportation, and enterprise IT trust Quantum to bring their data to life, because data makes life better, safer, and smarter. Quantum is listed on Nasdaq (QMCO) and the Russell 2000® Index. For more information visit **www.quantum.com**.

www.quantum.com • 800-677-6268

ST02349A-v03 Nov 2023