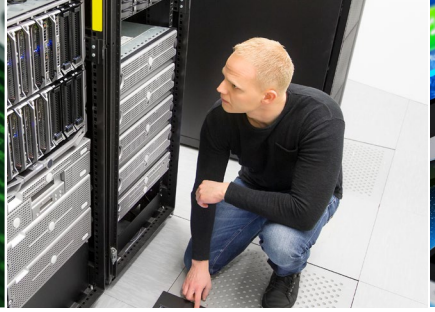
Quantum®

EXECUTIVE BRIEF:

BOLSTER YOUR IT DEFENSES TO MITIGATE COMPLIANCE RISKS AND PROTECT YOUR BRAND




Navigating New Threat Dynamics

Multiple organizations continue to fall victim to ransomware. This creates challenges for many C-level executives (CEO, CFO, CIO, CTO, CSO) because, while cyber threats are not very hard to predict, we know it's only a matter of time before one occurs—putting organizations at great risk. In heavily regulated industries—such as finance, government, education, and healthcare—negligent data security could result in hefty fines to the company, repercussions for board members, and financial harm to shareholders.

We have learned over the years that managing the fallout of a breach is not easy; it requires a heavy financial and workforce investment and disrupts business continuity. A breach at a major retailer in 2013 is a prime example of the long-lasting impacts that result when consumer data is not secured and protected. Post breach, many card holders vowed to stop shopping at the retailers' stores, which caused them to lose brand loyalty and damaged their reputation for years. In that instance, and for the first time in history, the CEO was ultimately relieved of their position with the company. While the retailer subsequently made significant improvements in data security, the issue prompted new, more strict regulations for every industry with which they interact. These adjacent businesses, just like their heavily regulated counterparts, face large penalties when they fail to prevent a data breach. Just like their heavily regulated counterparts, they too face large penalties when there is a failure to prevent data breaches.

Advanced Techniques to Bolster Your IT and Backup Environments

It is no secret that the best form of protection is to be proactive. Diligence is a must from top to bottom because ransomware can disrupt your entire organization with a single email at any level. In this executive brief, we'll explain how approaching ransomware recovery with a multi-layered strategy can help you protect your brand and avoid regulatory fallouts.

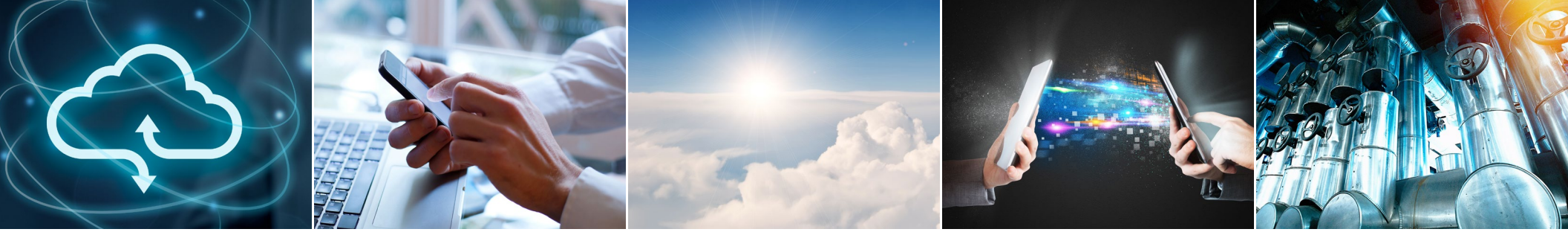
1. **Your reputation is priceless. Bolster your IT environment to protect your brand and stay compliant.**

2. **Think holistically.**

3. **Bolster your threat detection techniques against multi-stage threats.**

4. **Don't compromise your backups.**

5. **Determine the best multi-layered recovery method.**



1. Your reputation is priceless. Bolster your IT environment to protect your brand and stay compliant.

Your organization's data is priceless. Today it is the new oil, the new gold rush. Cyber criminals understand this, and they are wasting no time in stealing your data and attempting to destroy your reputation in exchange for ransom. This kind of attack on your business will cause damage to your reputation and loss of revenue, clients, and the trust it took you years to build—and will take you years to recover.

Don't let your brand suffer. Confidence in your brand will slowly recover, but the revenue will be gone forever, and your competitors will have widened their lead. If the value of your organization's brand and reputation are priceless, then having a proactive strategy to ensure all the controls are put in place is imperative.

Regulations are tightening to encourage companies to implement stronger data protection measures with the goal of mitigating victim impact. The General Data Protection Regulation (GDPR) and the California Consumer Protection Act (CCPA) were both put in place to provide significant financial consequences for privacy violations. Not only are the fines substantial, but with the CCPA, it is now easier for consumers to take legal action. So, what should your company do to protect itself?

→ Recommendation:
Implement an enterprise-wide prevention mechanism and protect your data.

An enterprise-wide prevention mechanism should be focused on backups, which are more critical than ever for the survival of cyber attacks. This will also help you meet regulatory guidelines, such as HIPPA, PCI, and any other industry mandates.



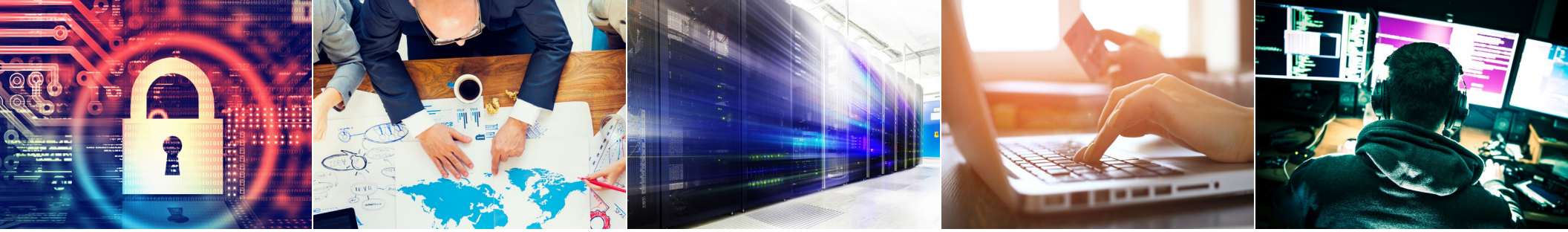

2. Think holistically.

Approaching a proactive strategy holistically allows you to see all possible points of entry and exit into your network, enabling you to see the weakest parts in the chain that can allow breaches. Part of the prevention process includes ensuring your IT teams understand your risk profile. Do they understand how data enters and leaves your environment?

→ Recommendation:
Reduce the surface footprint to your IT systems.

Reducing attack footprint/surface is critical, much like spring cleaning is to a winter-laden closet. Hardening your IT systems, or shutting down unnecessary features, needs to be heavily weighted against the benefits it produces. If those services can be disabled and gateway ports shut down, it might just stop the next successful attack.

Network protection and backups go hand in hand. If you are breached, your backups are going to be the primary way to get your business back online as quickly as possible, while your security teams run all the forensics to determine where your network was breached. Hence, why backups are crucial to a multi-staged threat.



3. Bolster your threat detection techniques against multi-stage threats.

We live in a digital economy where enterprises are constantly under attack and your backup data is coveted. Criminals are in reconnaissance, looking for weaknesses in networks across the world. They are leveraging artificial intelligence (AI) and machine learning (ML) to breach and disable your backup infrastructure, so you can't recover your data swiftly and get your business back online, which can cause damage to your reputation and customer trust.

→ **Recommendation:**
Master your protection software tools to detect anomalies in the network.

→ **Recommendation:**
Make sure your infrastructure is adhering to the best practice backup rule of 3-2-1-1.

Mastering protection software and analytic tools is imperative. Advanced analytical techniques, including AI and ML, can help detect abnormalities and vulnerabilities.

4. Don’t compromise your backups.

Attackers are now focused on your backup infrastructure. As your backup data is fast becoming the primary target, establishing security measures that protect your backup infrastructure becomes a critical component to address.

→ Recommendation:
Protect your data by tiering it to a non-network, immutable location.

A multi-layer approach can be a very cost-effective method to iron clad your data while keeping costs down. For any organization, backups are the lifeline that provides the business continuity should disaster strike. Tiering data to an immutable location, hopefully to a non-network addressable location, exposes less of your data and less of your reputation.

→ Recommendation:
Leverage the validation and verification tools available in backup systems.

Leverage the validation and verification tools available in the backup tools you employ to ensure that data being backed up is not corrupt. We suggest using a multi-layer approach because having two different validation tools within your backup infrastructure means that one can detect what the other has missed. These validation tools are available in a modern backup application as well as in the software included with disk, tape, and on-prem object storage.

5. Determine the best multi-layered recovery method.

→ Recommendation:
Implement a data recovery method in a storage tier that best suits your organization's environment.

Determine whether tape, disk, or cloud/object storage is the best recovery method for your organization.

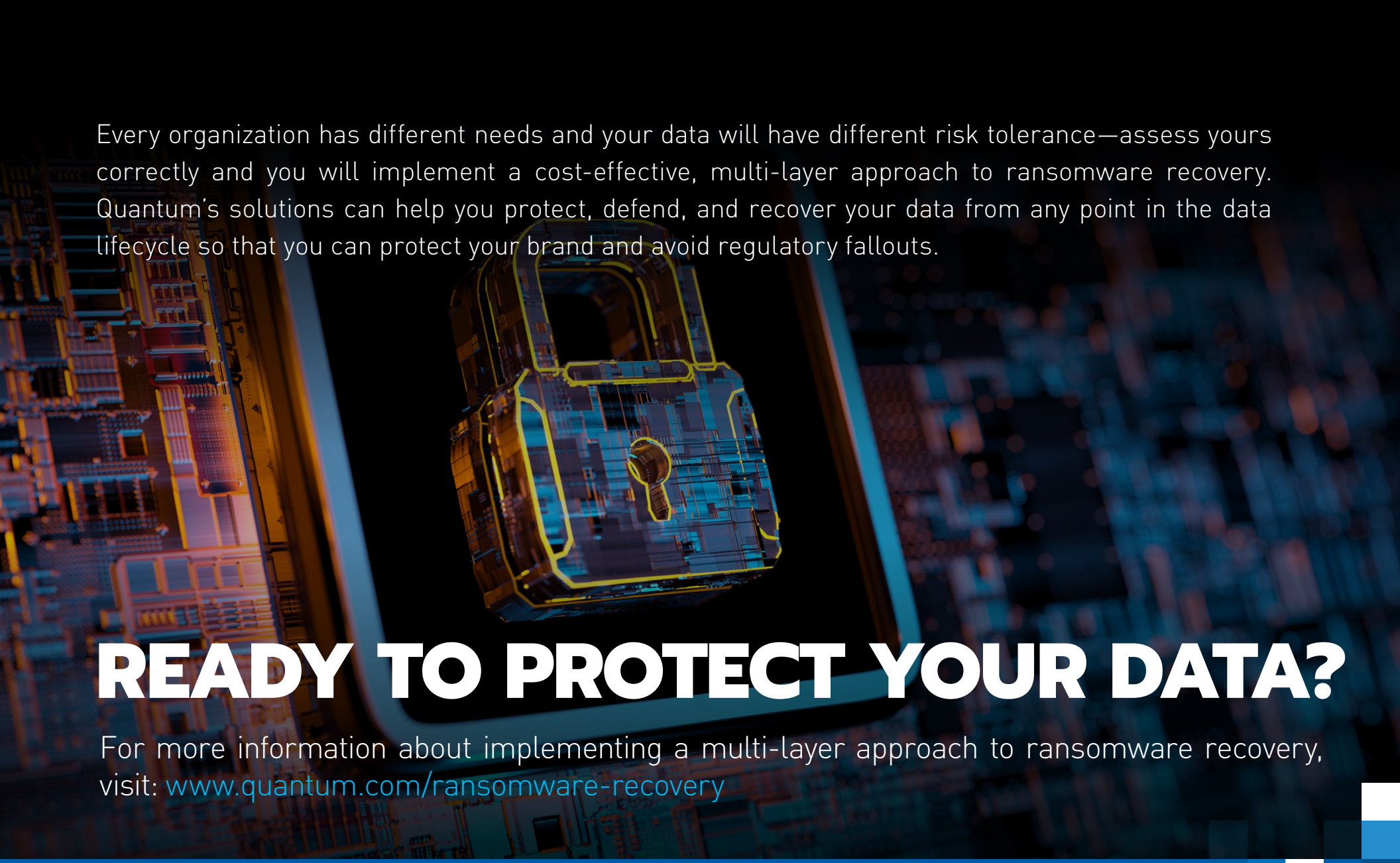
Low-Cost Retention Tier: It is a best practice to keep a copy of data in true, offline media—such as tape—in a multi-layer approach. Tape inherently provides physical air-gap protection, meaning it is not physically possible for a hacker to access it.

High-Performance Tier: Faster-performing tiers—such as flash, SSD, or HDDs—are a critical component to recover swiftly and to make data available when you need it.

Active Archive Tier: For storing large backup data sets for months or years, object storage creates immutable backups and is a scalable and cost-effective option for protecting valuable data against ransomware attacks.

Sources:
https://www.thehartford.com/resources/cyber/impact-ransomware-changing-regulation
https://www.varonis.com/blog/company-reputation-after-a-data-breach/

Every organization has different needs and your data will have different risk tolerance—assess yours correctly and you will implement a cost-effective, multi-layer approach to ransomware recovery. Quantum's solutions can help you protect, defend, and recover your data from any point in the data lifecycle so that you can protect your brand and avoid regulatory fallouts.



READY TO PROTECT YOUR DATA?

For more information about implementing a multi-layer approach to ransomware recovery, visit: www.quantum.com/ransomware-recovery

Quantum

Quantum technology and services help customers capture, create, and share digital content—and preserve and protect it for decades at the lowest cost. Quantum's platforms provide the fastest performance for high-resolution video, images, and industrial IoT, with solutions built for every stage of the data lifecycle, from high-performance ingest to real-time collaboration and analysis and low-cost archiving. Every day the world's leading entertainment companies, sports franchises, research scientists, government agencies, enterprises, and cloud providers are making the world happier, safer, and smarter on Quantum. See how at **www.quantum.com**.

www.quantum.com
800-677-6268

ST02355A-v01 June 2021