RSA

WHITE PAPER

Lessons from the Future of Cybersecurity

Focus on three key insights to protect against cyberattacks

Executive summary

Like humans, cybersecurity tends to be reactive. We react to a crisis and move on. But what if we changed that dynamic?

What if we imagined tomorrow's crisis, learned from it, and acted today?

By asking questions in three key areas, you can take advantage of major disruptions to foster future changes and accelerate innovation. Organizations should think deeply about constants, identify and focus on the imperatives, and ditch entrenched dogmas.

By focusing on these key insights, and reorienting their thinking to being identity-centric, leaders in every sector can move toward a more secure world.

OWN YOUR IDENTITY.

Humans tend to be reactive. People don't change until conditions force them to. Cybersecurity is no different. Because of limited time, resources, and bandwidth, we react to a crisis and move on. But putting out fires only addresses the symptoms, not the cause. But if you change that dynamic, imagining tomorrow's crisis, learning from it, and taking action today, you can better protect people, businesses, and the connections and data we rely on.

By tracing some of the conditions that could cause a cyber-crisis, you can determine what you need to do to keep up with changing technology, and the actions you must prioritize to protect vital information and infrastructures.

Disruption drives transformation

In the last few years, disruptions in the physical world have affected technology in general and cybersecurity in particular. For example, at the same time the global pandemic fundamentally changed how we live in the physical world, it created a more dangerous digital landscape. The number of cybersecurity complaints to the FBI Internet Crime Complaint Center spiked from 1,000 daily before the pandemic to as many as 4,000 incidents per day by April 2020.[1] The United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom's National Cyber Security Centre (NCSC) sent out an alert warning people that malicious cyber actors were taking advantage of COVID-19 fear and misinformation in phishing scams and exploiting vulnerabilities in new and often rapidly deployed remote access and teleworking infrastructure.[2]

The pandemic brought home the fact that we live in a hyperconnected world where the physical and digital are intertwined. Between 2019 and 2021, the number of reported ransomware complaints increased by 82 percent, and ransomware incidents were reported against 14 of the 16 U.S. critical infrastructure sectors.[3] In fact, 80% of critical infrastructure organizations experienced a ransomware attack in 2021.[4]

The Colonial Pipeline attack was an alarming example of the real-world effects of a ransomware attack against an industrial target and the impact it can have on people. All natural gas and most crude oil and refined products touch a pipeline, which means heating homes, powering cars, and plane travel all depend on the security of pipelines.

Colonial, one of the largest oil pipelines in the United States was hit by a ransomware attack by the DarkSide hacking group, which affected the billing systems and IT systems used to monitor the pipeline. Although the attack didn't affect the operational systems that transport fuel, Colonial shut down their pipeline operations until they confirmed the systems were safe.

The Colonial attack led to panic buying, which drove gas prices to hit a six-year high, resulted in massive lines at gas stations across the US, and even caused fuel shortages at military bases.[5,6,7] The Transportation Security Administration (TSA) released revised directives for pipeline owners and operators, beefing up requirements related to access control and credential management for critical infrastructure systems.[8]

Use disruption to your advantage

Because disruption in the physical world can shake our digital lives (and vice versa), leaders across government and the private sector need to build stronger foundations and smarter defenses.

And organizations are adapting. As a result of these new challenges, over the last few years many of the digital transformation projects that were initially 'nice-to-have' suddenly became 'we need it yesterday.' With telehealth use increasing 38X as compared to its pre-COVID baseline, an 1,885% growth in ransomware attacks on world governments, and hundreds of billions of dollars in additional e-commerce spending, organizations changed their priorities and budgets virtually overnight to accommodate new user behavior and to address new risks.[9,10,11]

But there is a silver lining to major disruptions; they can be an opportunity to foster change. Winston Churchill is credited with saying "never let a good crisis go to waste," and by asking questions in three key areas, you can use disruption to your advantage. You need to consider:

- **The constants.** What does not change?
- **The imperatives.** What matters most?
- **The dogmas.** What wrongly held beliefs should be tossed?

Using these three simple insights, you can learn and benefit from disruption.

1. Identify the constants

Although technology is enamored with change, constants are the basis for scientific progress. They provide an anchor you can use to build solutions. The pandemic is a case in point. When the world needed a solution to COVID-19 faster than traditional vaccine development could provide, research looked at the constant: the capabilities of the human body.

The mRNA technology in today's COVID vaccines uses the body to make proteins that look like the virus to train our immune system. The mRNA technology already existed for decades, but in 2020, the disruption of the pandemic was the impetus to look at the constants and combine it with key enabling technologies like nanotechnology. By taking advantage of a constant, vaccines were developed at warp speed.

In cybersecurity, there will always be new technology, new vulnerabilities, new exploits, and new malware that takes advantage of those exploits. Creating more resilient infrastructures, patching common vulnerabilities, and addressing exposures are positive actions we can take to mitigate these issues.

To be proactive, you need to recognize that while technology changes, certain things remain constant. To transform, we need solutions based on the one constant in cybersecurity: identity. According to Verizon, 82% of breaches involved human elements such as stolen credentials and phishing.[12] Most cyberattacks occur due to compromised identity and most attacks can be blocked by using multi-factor authentication (MFA).[13] In fact, cyber insurance providers won't sell you insurance unless you have MFA in place.

Much like mRNA, the underlying technology for MFA solutions has been around for decades. MFA was first commercially introduced in 1986, but despite its long history in cybersecurity, MFA usage remains shockingly low. In June 2021, only 2.3 percent of Twitter users had implemented two-factor authentication.[14] MFA implementation is only a little better in larger enterprises, where nearly 90% of cloud users had not implemented MFA, per a January 2021 study.[15]

Several barriers have prevented the widespread adoption of MFA, including the lack of open standards, the user experience, and the inertia of passwords. With the maturation of passwordless technology like FIDO and standards like Open ID Connect and SCIM, the need for passwords can finally end.

MFA should be adopted for every actor on the network, but even doing that is not enough. Organizations need to manage identity in a single, infrastructure-agnostic, independent platform that provides 360-degree coverage across authentication, access, authorization, lifecycle and governance of identities.

2. Understand the imperatives

In cybersecurity it's critical to know what's important and what's not. Disruptions have a powerful way to differentiate the mere important from the imperative. During disruptions, you focus on what matters most.

For example, in 1960, the Valdivia earthquake reached 9.5 on the Richter scale and left thousands dead. In 2015 another 8.4 disrupter shook Chile with several aftershocks at 7 and 6 plus, yet the death toll was less than 15.[16] Chile became the world's model for disaster and earthquake preparedness because of key insights that it had learned from the 1960 quake and implemented prior to the 2015 event:

1. Infrastructure damage and economic recovery are important, but the most important thing to protect during an earthquake is human life.

2. Earthquakes don't kill people; buildings and tsunamis kill people.

Chile systematically changed the building code and implemented a clear evacuation protocol, which reduced casualties by 100x.

In the context of cybersecurity, the imperative is protecting critical infrastructure and information. During the pandemic, CISA identified 16 sectors that we absolutely must protect, so people have access to basic needs such as food, water, healthcare, and transportation.[17] Although IT systems are important, they can be rebooted and replaced. If information is lost, it's irreplaceable.

Even more significant is when information is tampered with or distorted. In those situations, we get lost. Truth is another cybersecurity imperative. You need to know that the people accessing your systems are who they say they are, and that content that they produce is what it says it is. The best way to authenticate content is still authenticating the creator. Determining if a piece of information is true or not requires identifying the identity of the source of the information. Once again, identity must be verified and protected above all else.

3. Debunk the Dogmas

Disruptions debunk dogma and legacy thinking. When there are compelling reasons, people willingly give up conveniences. For example, at the time they were introduced, both seatbelts and children's car seats were considered inconvenient. But they saved lives, so people accepted them as worthwhile contributors to safe driving.

In cybersecurity, convenience has always been prioritized over security. It may not be convenient to use multi-factor authentication (MFA) to access systems, but the cybersecurity breaches from pandemic-related changes to work show why it matters. Just as those supposedly inconvenient seatbelts and car seats prevent death, 'inconvenient' MFA prevents breaches.

Digitization and the loss of any type of network perimeter mean it's time to stop sacrificing security at the altar of convenience. The goal should be security and convenience. Even governments are taking note of this change. In the United State, there has been an Executive Order related to cybersecurity and the Security and Exchange Commission (SEC) recently made moves to demand responsible disclosure and board governance of cybersecurity.[18,19] In 2021, Australia added the Critical Infrastructure Uplift Program (CI-UP), France released a new cyber alert system, and the UK government instituted vulnerability reporting.[20,21,22]

If governments and the private sector work together on both improving security and the user experiences, the side effect eventually may be innovations we haven't even thought of yet. It's time to ditch the dogma of security or convenience. Today, cybersecurity goals should be reframed to focus on security and convenience and innovative benefits.

Moving forward after the crisis

Nobody enjoys living through crises, but we can learn from them. In cybersecurity, the pandemic has lessons to teach us as we move forward into the future:

1. Identity is the one constant we can count on in the ever-changing world of technology.
2. The truth is what matters most and what we need to protect. The veracity of information is critical.
3. In a contest between convenience and security, security should always win.

Learning from the most recent disruption can help prevent a cybersecurity-related crisis in the future. Although a cyber crisis may not cost as many lives as COVID-19, it would spread much more quickly. If it takes out critical infrastructure, a cyber crisis could have massive and debilitating economic and societal impact. When the physical world was disrupted by a virus, we shifted online to remain productive and connected. But if the digital world were disrupted, what would happen? What would we do?

Transforming security in a work-from-anywhere world

Transforming security requires reorienting our thinking from being infrastructure-centric to identity- and information-centric. To do that, organizations need to think deeply about constants, identify and focus on the imperatives, and ditch entrenched dogmas. The cybersecurity industry needs to transform. Our survival may depend on our ability to learn from past experiences and apply those lessons to future initiatives.

With people regularly connecting from beyond the traditional secure network perimeter, using a variety of devices and platforms, and relying on those connections for everything from food to fuel to healthcare, security needs to change. It should be just as easy to authenticate whether someone is using a corporate-issued laptop or personal device. Solutions need to support a broad range of modern authentication methods to accommodate both the organizations and user's preferences and circumstances.

Authentication needs to work all the time, every time, to keep people connected and productive whether they're connecting to the cloud or on-premises. Technology should have documented high availability features and have options for other ways to stay connected to the cloud even when internet connectivity is disrupted. Identity and access management should be easy for admins to ensure appropriate levels of access, with visibility into access across blended cloud and on-premises deployments.

Learn more about RSA identity and access management solutions at rsa.com

About RSA

RSA provides trusted identity and access management for 12,000 organizations around the world, managing 25 million enterprise identities and providing secure, convenient access to millions of users. RSA empowers organizations to thrive in a digital world, with complete capabilities for modern authentication, lifecycle management and identity governance. Whether in the cloud or on-premises, RSA connects people with the digital resources they depend on everywhere they live, work and play. For more information, go to RSA.com.

1. "FBI sees spike in cyber crime reports during coronavirus pandemic," The Hill April 16, 2020. https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic/
2. "COVID-19 Exploited by Malicious Cyber Actors," CISA, April 8, 2020. https://www.cisa.gov/uscert/ncas/alerts/aa20-099a
3. "FBI Partnering with the Private Sector to Counter the Cyber Threat," FBI, March 22, 2022 https://www.fbi.gov/news/speeches/fbi-partnering-with-private-sector-to-counter-the-cyber-threat-032222
4. "Ransomware attacks, and ransom payments, are rampant among critical infrastructure organizations," Help Net Security, February 10, 2022. https://www.helpnetsecurity.com/2022/02/10/critical-infrastructure-ransomware/
5. "Panic Drives Gas Shortages After Colonial Pipeline Ransomware Attack," NPR, May 11, 2021. https://www.npr.org/2021/05/11/996044288/panic-drives-gas-shortages-after-colonial-pipeline-ransomware-attack
6. "Gas hits highest price in 6 years, fuel outages persist despite Colonial Pipeline restart," ABC News, May 17, 2021. https://abcnews.go.com/US/gas-hits-highest-price-years-fuel-outages-persist/story?id=77735010
7. "Some military bases limiting gas purchases, encouraging telework in wake of pipeline shutdown," Military Times, May 11, 2021. https://www.militarytimes.com/pay-benefits/2021/05/11/some-military-bases-limiting-gas-purchases-encouraging-telework-in-wake-of-pipeline-shutdown/
8. "TSA revises and reissues cybersecurity requirements for pipeline owners and operators," TSA, July 21, 2022. https://www.tsa.gov/news/press/releases/2022/07/21/tsa-revises-and-reissues-cybersecurity-requirements-pipeline-owners
9. "Telehealth: A quarter-trillion-dollar post-COVID-19 reality," McKinsey & Company, July 9, 2021. https://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/telehealth-a-quarter-trillion-dollar-post-covid-19-reality
10. "There's a huge surge in hackers holding data for ransom, and experts want everyone to take these steps" Fortune, February 17, 2022. https://fortune.com/2022/02/17/ransomware-attacks-surge-2021-report/
11. "Coronavirus pandemic adds $219 billion to US ecommerce sales in 2020-2021," Digital Commerce 360, March 15, 2022. https://www.digitalcommerce360.com/article/coronavirus-impact-online-retail/
12. "2022 Data Breach Investigations Report," Verizon. https://www.verizon.com/business/resources/reports/dbir/
13. "Tech CEOs: Multi-Factor Authentication Can Prevent 90% of Attacks," Infosecurity Magazine, September 3, 2021. https://www.infosecurity-magazine.com/news/tech-execs-mfa-prevent-90-of/
14. "Why Are Users Ignoring Multi-Factor Authentication?" Security Week, "July 27, 2021. https://www.securityweek.com/why-are-users-ignoring-multi-factor-authentication
15. "Statistics Warn About the Urgent Need for MFA" Systems Engineering, January 21, 2021. https://blog.systemsengineering.com/blog/new-statistics-warn-about-the-urgent-need-for-mfa
16. "How did Chile manage to survive its recent earthquake virtually unscathed?" The Guardian, September 2015. https://www.theguardian.com/cities/2015/sep/25/how-chile-survive-earthquake-virtually-unscathed
17. Critical Infrastructure Sectors, CISA. https://www.cisa.gov/critical-infrastructure-sectors
18. "Executive Order on Improving the Nation's Cybersecurity," The White House, May 12, 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
19. "SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies," SEC, March 9, 2022. https://www.sec.gov/news/press-release/2022-39
20. "Critical Infrastructure Uplift Program," Autrailian Cyber Security Centre. https://www.cyber.gov.au/acsc/view-all-content/programs/critical-infrastructure-uplift-program-ci
21. "France: Ministry releases new system to notify of major cyber incidents," Data Guidance, August 3, 2021. https://www.dataguidance.com/news/france-ministry-releases-new-system-notify-major-cyber
22. "Vulnerability Reporting," National Cyber Security Centre. https://www.ncsc.gov.uk/information/vulnerability-reporting

RSA