Cyolo

2022 CYBERSECURITY REVIEW
LESSONS FOR THE YEAR AHEAD

INTRODUCTION

The stats are in, and it has never been clearer that cyberattacks present a real and present danger to the enterprise world and the general public alike.

Just a few notable findings from **IBM's 2022 Cost of a Data Breach Report**:

A data breach in the U.S. costs over twice the global average.

It takes an average of 277 days to identify and contain a breach.

Nearly half of all data breaches happen in the cloud.

Stolen or compromised credentials were the most common cause of data breaches and took the longest time to identify.

The share of breaches caused by ransomware grew by 41%.

While **the education, research, healthcare, and government sectors** face a particularly heavy volume of attacks, no company or industry is invulnerable. If 2022 proved anything, it's that the nature and implications of cyberattacks can run the gamut.

As the world looks to accommodate the demands of global digital transformation—remote work, increasingly complex landscapes, a widening gulf between legacy and modern systems—it's worth taking the time to draw some inferences from the past 12 months of cyberattacks.

SUPPLY CHAIN ATTACKS COMPROMISED BIG-NAME BRANDS

PUMA

In January, international sportswear and lifestyle brand **Puma suffered a data breach** following a ransomware attack on one of its suppliers—Kronos, which provides a suite of solutions for scheduling, attendance, payroll, and other workforce management solutions.

Attackers breached the Kronos Private Cloud environment and stole personally identifiable information (PII) of more than 6,600 Puma employees.

OKTA

Even identity providers aren't immune to becoming a single point of failure for their customers.

Notorious hacker group Lapsus$ **compromised Okta's systems in January** by gaining remote access to a machine belonging to a third-party customer service vendor. In fact, the machine belonged to an employee of a company that Okta's vendor had just acquired.

CVS

A CVS database hosted by a third party was discovered to have **no form of authentication whatsoever** to prevent unauthorized entry. The database exposed more than 1.1 billion customer email addresses, user IDs, and customer searches on CVS Pharmacy websites.

Not only is there a risk for customer searches to be triangulated with the Session ID to determine the identity of a searcher, but the exposed email addresses may be used in a larger phishing campaign.

THE TAKEAWAY

Dependence on third-party vendors is simply the reality of today's enterprise world, but these and other similar incidents shatter the illusion that vendors are inherently trustworthy.

Extending security controls into the unknown environments of vendors, downstream suppliers, and acquired systems can be impossible. Instead, organizations should adopt a "never trust and always verify" approach to vendor security and execute that approach by enforcing zero-trust access for all third-party users.

THE TENSION BETWEEN USABILITY AND SECURITY ELEVATES RISK

RONIN

Every online gaming developer dreams of producing the next *Fortnite* or *Among Us*.

Ronin's game, *Axie Infinity*, added a financial element of digital currency and NFTs (Non-Fungible Tokens) that players can earn as they play. As the game grew in popularity, Ronin scaled back its security controls so its servers could accommodate increased traffic. Unfortunately, criminals slipped in among the gamers and **stole $625 million in cryptocurrency.**

SAMSUNG

Whatever else you can say about Lapsus$, they certainly had a busy year. The group hacked **vital Samsung data, including source code** for a range of functions, along with algorithms for biometric authentication. Lapsus$ then made the 190 GBs of data publicly available through a file-sharing site.

ROCKSTAR GAMES

In September, **a lone teenage hacker breached Rockstar's servers** and stole source code for Grand Theft Auto V, Rockstar's most popular game and the second highest-selling game of all time.

The attacker then attempted to sell the code through Telegram. If successful, pirates would gain the ability to manipulate the online version of the game and seriously compromise its functionality.

THE TAKEAWAY

Organizations need to ensure usability for both business users and end users at scale, but they must also work to make security just as scalable. As the Ronin breach shows, organizations will be forced into a lose-lose situation if they have to choose between usability and security: miss out on revenue or suffer the financial cost and reputational damage of a breach.

In the case of Samsung and Rockstar, it is clear that to innovate at the speed demanded by the market, developers need convenient access to sensitive assets like source code and production environment; however, it is equally critical that this access be controlled in a way that does not permit security to be compromised. Zero-trust access to assets rather than the full network, along with enforcement of the principle of least privilege, helps ensure that developers maintain productivity without exposing their companies to extra risk.

ATTACKS ARE CROSSING OVER INTO THE PUBLIC SPHERE

MARYLAND DEPT. OF HEALTH

The Maryland Department of Health (DoH) **suffered a ransomware attack** in December of 2021 that lasted into the next year.

The attack took down many of the state health department's web pages, including pages that allowed Maryland residents to apply for Medicaid, order at-home tests, and other functions. As a result, the DoH couldn't report COVID-19 data for nearly two weeks.

SPICEJET

The second-largest airline in India with over 102 aircraft, **SpiceJet suffered an attempted ransomware attack** that disabled much of its website in May.

Though SpiceJet's IT team acted quickly and largely contained the attack, the disruption caused a "cascading" effect on SpiceJet's flight schedules, leading to delays, irate customers, and heavy financial losses.

MARQUART & BAHLS

Two subsidiaries of the German logistics giant were attacked in February, disrupting IT systems and causing over 200 gas stations across Germany to close. Both subsidiaries declared force majeure for most of their inland supply activities in Germany.

As climate change, the war in Ukraine, and other geopolitical factors heighten volatility, it's a safe bet to expect more attacks on energy providers.

THE TAKEAWAY

Critical infrastructures like healthcare, energy, and transportation are always on and running at high capacities— which makes these systems tough to secure and even tougher to modernize. This is precisely why they are becoming more frequent and lucrative targets for threat actors and hacker groups. Even the smallest disruption in these systems can cause significant loss of business or even life.

Organizations must work to extend modern, robust security and access controls to their legacy systems and applications to protect the public and the global economy, in addition to their own businesses.

CYBER WARFARE IS STILL UNIQUELY HUMAN

VERIZON

In October, an unidentified attacker **compromised around 250 prepaid wireless accounts**.

The attacker posed as a customer service representative and convinced Verizon store employees to change the device's phone number to a SIM card controlled by the hacker. This type of "SIM-swapping" theft occurs across carriers and sometimes involves bribed employees. While the number of accounts affected is small, the method bears noting.

UBER

Uber's internal servers were breached after a contractor's device was infected with malware and login credentials were sold on the dark web.

The hacker spammed the contractor with a stream of approval requests, also known as "MFA-bombing," until the contractor accepted one of the requests. Then the hacker accessed several other employee accounts, granting themselves higher permissions to tools like Slack and the company's G Suite.

CASH APP

In April, Cash App discovered that an **ex-employee downloaded a report containing a significant amount of customer data**. The report contained names, portfolio values, stock trading information, and brokerage account numbers associated with Cash App Investing.

The ex-employee didn't hack into Cash App's customer database. Their access was simply never revoked once they left the company.

THE TAKEAWAY

Bad guys don't break in; they login. These breaches weren't sophisticated manipulations of powerful technology; the attackers merely took advantage of human gullibility, rash decision-making, and neglect of protocol.

It's a demonstrable fact that humans are easier to compromise than systems. This is why weak and stolen password enable the vast majority of hacking incidents, and **phishing scams are still the most common form of cyberattack**, according to the FBI.

The most hardened network defenses can be undone with a single errant click or poor decision by a busy team member. This is not a judgment; it is simply a reality. And let's face it, with remote and hybrid work now widespread and seemingly permanent, perimeter-based security has, at last, breathed its final breaths. Today, **people are the network perimeter,** and organizations of all types must implement access controls like multi-factor authentication (MFA) and single sign-on (SSO) to secure workers themselves rather than their networks.

WHERE DO WE GO FROM HERE?

If these attacks can teach us anything, it's that any vulnerability can be exploited and no organization is too big to be breached. Tried-and-true approaches of the past simply no longer hold up. To operate with confidence in the coming years, organizations must accept new realities and seek innovative solutions to solve their security challenges.

EMBRACE ZERO-TRUST

The **zero-trust security framework** shifts the attributes of validation from network-based parameters, like originating network and domain membership, to identity-based parameters, like biometrics, digital signatures, and public key cryptography. Under zero-trust, every device, user, and identity is verified and then continuously authenticated before access to any corporate asset is granted.

This approach offers two significant advantages over the traditional "castle and moat" approach:

ZERO-TRUST MEANS ZERO.

No user or device is inherently trusted, whether an access request is coming from inside the corporate network or from the CEO's cell phone. And beyond the initial user verification, which should ideally include MFA, continuous authentication runs in the background to detect unusual or anomalous activity. A top-of-class zero-trust access solution will include real-time session monitoring and give administrators the ability to end a session (effectively shutting the user out of the system) if suspicious behavior is detected.

ZERO-TRUST PROVIDES ASSET ACCESS INSTEAD OF NETWORK ACCESS.

In the perimeter-security model, which virtual private networks (VPNs) continue to follow, users are authenticated once and then generally given access to the entire network. This means that if a nefarious actor gains access, they could feasibly wander through the system until they find the assets they're after. In the zero-trust model, by contrast, users receive access only to the assets they need for their jobs, according to the principle of least privilege. So, even if an attacker did find a way in, they would not have full network access and would be substantially less dangerous.

MINIMIZE THE BLAST RADIUS

The zero-trust approach actually assumes by default that attackers are already inside the system. The emphasis is, therefore, on giving bad actors no room to roam and minimizing the potential harm they could cause.

The following activities and policies can help limit an attacker's ability to do damage:

ENFORCE THE PRINCIPLE OF LEAST PRIVILEGE

Managing permissions across the enterprise can be tedious, but it is an important job. Without properly-tailored roles and permissions, suspicious behaviors are harder to detect. Plus, even well-meaning employees can accidentally cause harm when given free rein to the corporate network.

Each organization must intimately understand its use cases and design its permissions in a way that accurately supports and reflects the workflow of each role.

For the initial zero-trust implementation, Cyolo recommends dividing the project into three stages based on user groups and access levels:

- **High-risk users**, including third-party vendors and employees who access critical infrastructure
- **Remote users**
- **Hybrid and on-premises users**

GAIN VISIBILITY INTO CONFIGURATIONS

Cloud usage comes with an endless stream of vulnerabilities, like unsecured credentials, network exposures, and at-risk workloads. Teams need a hub for centralizing and maintaining cloud configurations so that nothing falls through the cracks.

SEGMENT NETWORKS

Instead of having one universal network, breaking the network down into compartmentalized sub-networks gives security teams more dexterity in tailoring access and more precision in shutting out bad actors. As a bonus, different segments can be designed to accommodate mobile devices, clouds, and other systems that demand more nuanced network virtualization and provisioning.

IDENTIFY UNUSUAL ACTIVITY

Bad behavior is almost always preceded by unusual behavior. Organizations with limited visibility into network activity and sub-par protocols for dictating access parameters will find themselves on their back foot when a breach occurs. Zero-trust access solutions take contextual behavior into account when validating identity.

CREATE A PLAYBOOK

Organizations can't wait until an attack occurs to decide how they will handle it. Different teams and team members must know what to do in the event of a breach or attack, from shutting down critical systems to making public statements and responding to angry customers.

CYOLO AND REAL ZERO TRUST

As we have seen, even the biggest names in cybersecurity are susceptible to cyberattacks. Okta, the market leader in identity management, was **breached four times in 2022**. LastPass's catastrophic breach keeps getting worse **as more information surfaces**.

When it comes to zero-trust network access (ZTNA) vendors specifically, the paradox is that the majority don't provide real zero-trust access. As a customer, you're still forced to trust one entity — the ZTNA vendor. Trust isn't eliminated, it's simply consolidated in a single vendor who is, ostensibly, a better custodian of access keys than business users. But, as an endless string of breaches shows, no one is invincible.

Real zero trust creates better keys, rather than simply creating a new, centralized key holder. Real zero trust gives everyone a unique key that can't be forged or compromised by another person, including the ZTNA provider.

Cyolo is the only platform that offers a single-click true zero-trust access experience that delivers business users directly to the applications and assets they need to work and saves them from login fatigue.

Unlike other ZTNA vendors, Cyolo has no visibility to customer passwords or assets and, therefore, cannot become a single point of failure.

With Cyolo, organizations can also easily extend MFA and SSO to remote workers, third-party vendors, legacy applications, and other challenging use cases without a drastic, costly rip-and-replace.

As we embark on 2023, organizations can't afford to choose between security and business agility. To meet the threat landscape of tomorrow, security must contribute to innovation rather than stand in its way. Zero-trust access is the way forward.

Cyolo

ABOUT CYOLO

Too many critical assets and systems remain exposed because traditional secure access solutions are not able to protect the high-risk access scenarios and legacy applications that keep business operations running. Cyolo provides the fastest and most secure Zero Trust Access (ZTA) solution to give organizations visibility and access control over the users who leave them most exposed to risk, including third-party workers, remote OT operators, and post-M&A employees and applications. Founded by a CISO and two ethical hackers, Cyolo solves one of the highest stakes challenges in cybersecurity and gives security leaders the controls they need to enable their business.

cyolo.io