SCTE CABLE-TEC EXPO FAST FORWARD 2021
VIRTUAL EXPERIENCE
OCTOBER 11-14

2021 Fall Technical Forum
SCTE • NCTA • CABLELABS

From Bolted-on to Built-in: The Journey of Cybersecurity

A Technical Paper prepared for SCTE by

Casandra Bowes
Principal Security Architect
Comcast
650 Centerton Road, Moorestown, NJ 08057
(609) 313-5636
casandra_bowes@comcast.com

Harwant Mahal
Director, Security Authentication and Access Management
Comcast
650 Centerton Road, Moorestown, NJ, 08057
(215) 756-4387
harwant_mahal@comcast.com

Table of Contents

Title **Page Number**

List of Figures

Title **Page Number**

1. Introduction

Over the past two decades, the transformation of service delivery and use of social media and digital platforms have opened the flood gates for the threat landscape. When it comes to protecting ourselves from bad actors, are tips, tricks, and risk indicators enough?

In short, the answer is no. It is not enough in some cases. We see evidence of this every day in the news. Even though we see signs that bad actors are sometimes successful, security professionals often prevail. With a conscious effort to move from "information" and "education" to meaningful behavioral change, we are turning the tides.

Laws are being written and updated with new mandates on data protection and privacy. Corporations are taking strides, reacting to government mandates, and implementing initiatives such as shifting security left. Security professionals are stepping up their game on both user and device identity, reducing the blast radius of potential attacks, and making it harder for bad actors to breach networks and steal data. Protection is provided to consumers by building security into products and services, as well as account protection measures like strong authentication and alerts of new or suspicious activity.

But there is more to do. Security professionals must go beyond tips, hacks, and risk indicators and use all the tools in their arsenal to create plans that incorporate a blend of policy, process, and technology as a catalyst to change end-user and consumer behavior.

This paper demonstrates how security threats have shifted marketplace adaptation. Modern DevSecOps and security practices are discussed, along with how establishing cyber risk ratings to provide accurate and transparent cyber health can uplift security efforts. Adoption of these transformations can bring security out of the shadows and benefit corporations and consumers alike, making a siloed approach to security tenable.

2. Security Goes Mainstream

The 2010s can be labeled as the decade cybersecurity went mainstream. Data breaches started to make big headlines. Personal information was being stolen from big name retailers, popular gaming sites, and even the US government. Millions of people were affected, and corporations faced extensive downtime, costly damage, expensive fines, lawsuits, and a loss of consumer trust. Government secrets were exposed, threatening the safety and security of nations. The lives of everyday people were being affected by cybercriminals and it was being felt across the globe.

2.1. How Hackers Pushed Security Forward

Cybercriminals with no budget constraints or change control processes developed a level of sophistication that surpassed the outdated "point solution" security controls that were protecting our most valuable data. They were taking a multifaceted polymorphic approach that easily bypassed the mechanisms that were supposed to keep them at bay.

Amidst all the damage, society was awakened to just how much disruption and destruction could be done with surprisingly little effort. This changed the perception that security can be left as an afterthought. Cybersecurity budgets grew. Corporate board members started paying attention. Governments started paying attention. Consumers started paying attention. Security was getting its long overdue 15 minutes of fame.

While there is no industry that is safe from the threat of attack, the cable industry is one of the top 10 targets for hackers [1]. "Always-on" internet access and video streaming have changed consumer behavior. Consumers are moving away from watching linear channels to adopting streaming channels which require high-speed broadband. With this shift in demand, broadband security risks are being compounded. As the details and motivations of attacks continue to evolve, there are several popular methods attackers use, which are described next.

2.1.1. Compromised Accounts

A favorite weapon of choice when looking to gain unauthorized access to networks and wreak havoc on unsuspecting victims is compromised accounts. Companies can see from hundreds to thousands of attempts per day to penetrate both enterprise and consumer accounts on their networks via compromised credentials. Due to increased sophistication of password-related attacks, coupled with the slow adoption of methods to combat them, an astounding 61% of data breaches can be traced to compromised credentials. [2] There are several ways in which accounts are compromised. Some of the more common methods include phishing attacks, brute force password attacks, and credential stuffing.

Once an attacker retrieves a set of credentials, they are validated, and after a successful test, made available on the dark web for sale. Fraudsters then purchase these credentials and use them not only to access consumer broadband accounts and steal services, but also as a pivot point to identity theft. Additionally, the fraudsters can sometimes use the credentials to access consumer email. Once access to an email account is gained, they use scanning tools to find third party targets like bank information, financial transactions, credit card information or crypto currency accounts associated with the victim. The email credentials are used to reset passwords, and possibly as 2nd factor authorization to access the victim's financial accounts. Sometimes fraudsters can even get as far as transferring money out of a victim's account. The use of stolen credentials by fraudsters to gain access to consumer banking services creates a ripple effect to the financial sector. Though cable operators can implement more secure authentication mechanisms to protect their own subscriber accounts, a chain is only as strong as its weakest link. If authentication is weak on one account, all accounts that are linked are exposed to risk.

The use of video streaming services by consumers during the pandemic has increased many folds. Some consumers share their credentials with their family, but in some cases, these credentials are sold for commercial use. The identification of legal sharing of passwords within family or illegal sharing has become another threat to video streaming and account security.

2.1.2. Brand Phishing

"Lower your cable bill" is an example of a scam that has been around for many years and has hurt the brands of many cable companies. The scammers pose as 'companies' officially doing business, call customers, and trick them with better deals, getting monthly payments out of their pockets and impacting the company brand. Often, these scammers will request the account credentials to offer discounts, further exposing the subscriber to identify theft risks.

2.1.3. Ransomware

Ransomware attacks go beyond just stealing and exploiting data, with recent attacks impacting the daily lives of many in ways we have not experienced before, causing gas shortages, interruptions in public transit, and disrupting the food supply chain. Unfortunately, experts do not expect this onslaught of attacks to slow down anytime soon. It is projected that during 2021, ransomware attacks against business will occur every 11 seconds, with costs expected to exceed $20 billion globally. [3]

The concept of a ransomware attack is as follows: The hacker finds a way to install malicious software onto an unsuspecting network. Usually this occurs via malicious emails with malware, an unpatched vulnerability, or exposed ports or services with weak authentication for remote access. Once the ransomware is deployed, the data is encrypted, and the victim receives a ransom note demanding payment, usually with a cryptocurrency such as Bitcoin. The victim is then faced with the choice to either pay the fee or incur the untold damages of downtime, rebuilding, or declaring a total loss on the infected resource(s). When faced with these difficult options, more than half of the victims of ransomware attacks pay the ransom. This is not a favorable outcome, given that it fuels further ransomware attacks.

2.1.4. Voice Fraud

Voice technology has taken a strong position in customer interactions for businesses in recent years. It is the future of every service offering and still being adopted in the industry. The voice interactions are using artificial intelligence (AI) for chat bots to respond to customers. There are device apps which provide faster calling services. These new innovations in voice technology have invited scammers for voice phishing [4] [5]

Additionally, scammers make their way into unsuspecting victim's voice service accounts and place high volumes of expensive calls on the victim's dime. This practice is lucrative for criminals and expensive for voice service providers with an estimated cost of $12 billion dollars in damages annually.

2.1.5. Internet Facing Application Attacks

Business-centric interactive websites have become the new norm to do business and provide quick responses to customers. Although these on-line sites have tremendously

improved the user experience, they have also brought new cyber security threats. The most common threats are on web servers and databases for cross-site scripting and SQL injection. According to industry data, 90% of the applications have security flaws and it takes an average of 38 days to patch the application-related components. During the development process of these web applications, code analysis is done for less than 50% of applications. [6] A small rogue application, which is not on a company's radar, poses an even larger risk due to lesser controls and assessments. A vulnerability on a rogue application's web server with internet connectivity and unknown change control practices, can invite a threat actor with this ingress and allow lateral movement.

2.2. Turning the Tides

If there is one guiding principal security professionals should follow, it is this one: Assume you will be breached.

Most companies have started initiatives related to the overall cybersecurity uplift, to strengthen the ingress points, decentralize applications, implement, and govern the security frameworks with Zero Trust to reduce the blast radius -- to name a few. The use of Machine Learning (ML) for cybersecurity threat intelligence, multi-factor authentication to inform risk engines, for both users and devices, has contributed greatly to the understanding and reduction of risk within the threat landscape. The enterprise-side user education on threats, via ransomware readiness exercises, phishing exercises, and Zero Trust programs will help prepare the organizations for growing attacks. The implementation of MFA brought a positive change, and over last couple of years it reduced the number of threats for identities.

2.2.1. Zero Trust Security

If one were to make a list of most popular security buzzwords, Zero Trust would likely be close to the top. But while buzz words usually get a bad rap with security professionals for not living up to the hype, Zero Trust would be an exception. Maybe because Zero Trust is more than a "latest and greatest" product suite that you enable to solve all your security woes. In fact, it's not a product at all, but rather a philosophy or mindset of "never trust, always verify." [7] [8]

Traditional security models worked like a "castle and moat" system for accessing corporate resources. A perimeter was created around the company network and security efforts were focused on ensuring the perimeter was not breached. Everything within the perimeter was considered a safe and trusted resource. Everything external to the perimeter was not trusted. This model was more effective when corporate resources lived within the perimeter and were accessed from the confines of the corporate network using corporate owned devices. Today this is not the case. Corporate resources exist both within and external to the corporate network and can often be accessed from any device and/or location. The network perimeter, where security efforts were traditionally focused, has disappeared. [9]

In contrast, a zero-trust security model assumes every device, user, and application is a threat until verified. Every resource is treated as though it is an attack vector, and measures are taken to contain the damage of an attack. IP based access controls are replaced with identity-based controls and security is taken out of the shadows by shifting the focus to people, devices, and applications as the network perimeter.

While each organization will implement a zero-trust security model in its own way, there are common elements that one would expect to find including strong identity management for users, devices and applications, network segmentation, and advanced monitoring and logging. [10]

2.2.2. Improved Incident Detection and Response

To stay ahead of the constantly shifting threat landscape, corporations are building their own threat intelligence programs. These programs, focused solely on threat prevention and detection, use a combination of threat intel data collected from trusted sources and advanced SEIM technologies to alert organizations of potential and actual threats. They also focus on incident preparedness, using tools such as the MITRE ATT&CK framework.

The MITRE ATT&CT framework was designed to help organizations in assessing risk against common tactics used by attackers. The framework is defined as “a comprehensive matrix of tactics and techniques used by threat hunters, red teamers, and defenders to better classify attacks and assess an organization's risk” [11]. Using tools such as the MITRE ATT&CK framework can assist with mapping threats detected in a SEIM system to potential use cases for security automation.

Another instrumental tool in preparing for attacks is an exercise known as a purple team event. In these events, both a red team (made up of “attackers”), and a blue team (made up of “defenders”) get together in a controlled environment and use an “offensive defense” strategy to identify security gaps within an environment. These exercises, sometimes partnering with specialized third-party organizations, help to improve skills and techniques of the participants so they are ready to respond when a real incident occurs. They also bring visibility to security gaps that do exist, which helps prioritize the efforts of resources so they can focus on the biggest wins.

2.2.3. Multi Factor Authentication

We already know that one of the most common ways data breaches occur is compromised credentials. We have also looked at common ways accounts are compromised. The best defense against these kinds of attacks is the use of multi factor authentication (MFA).

The premise of MFA is that you prove you are who you say you are – aka authenticate yourself - by providing something you know – your password – with something you have

(token, one time passcode [OTP], approved sign-in request) and/or something you ARE (fingerprint, facial recognition).

Although some forms of MFA have been around for the better part of two decades, adoption has been slow, mostly due to cost, additional hardware requirements, and the cumbersome user experience. Prior to the abundance of data breaches that took place over the past decade, companies and consumers alike were not particularly interested in investing money or losing convenience by adding steps to access online resources. As companies grew better at detecting compromised accounts and realized how often and easily passwords were being compromised regardless of "best practice" password policies, it became widely recognized that the benefits of MFA far outweighed the drawbacks of cost and inconvenience.

Technical difficulties, conflicting priorities, and an endless list of ever-changing use cases are just a few of the very real challenges companies may face when deploying an MFA solution, especially when considering the vast differences between protecting enterprise and consumer accounts. However, there is no disputing its effectiveness at stopping password related attacks almost entirely, with a success rate of more than 99% [12].

When implementing MFA, there are a variety of different solutions from which to choose. Depending on the complexity of the environment, there may not be a single solution that meets all use cases. In situations such as this, multiple solutions may need to be deployed to ensure all resources and users are MFA protected. For many companies it is likely that MFA will be an ongoing journey that will continually be improved upon as new technologies emerge to combat the ever-constant threat of account takeovers.

2.2.4. Ransomware Readiness

With ransomware attacks on the rise, it is more important than ever to be prepared on how to respond to a ransomware attack. There is no one single strategy to combat ransomware attacks. To best prepare for a successful outcome, consider the below recommendations:

a) Address your known vulnerabilities and keep up to date on patches, especially on parameter assets.
b) Disable unused services and processes, specifically remote desktop protocol (RDP) and secure shell (SSH), on externally facing systems. If these services must be exposed, use access control lists (ACLs) and multi-factor authentication.
c) Use least privilege access models.
d) Reduce the blast radius of attacks with network micro segmentation
e) Use advanced security tooling for logging, monitoring, and alerting to bring visibility to what's happening within your environments
f) Back-up your systems regularly and encrypt backups
g) Have a response plan ready and practice recovery efforts, especially for critical resources.

2.2.5. Shifting Security Left

The concept of "shifting security left" is all about closing security gaps further upstream. To accomplish this, security feedback must be incorporated as part of the feedback loop throughout the entire software development lifecycle (SDLC). Adopting the mindset of addressing security concerns before any code is written saves teams considerable time and money and elevates the level of trust customers have in products and services. When a multifaced approach is taken that includes training, coaching, and automation to help prioritize the sometimes-overwhelming number of security tasks, application development teams can improve the chance of successful delivery for secure products without adding any additional time to their development cycles.

The software development cycle has many skip hops when trying to reduce cycle time and get products delivered faster into customer hands. To support shortened cycle times that incorporate security into the development process, many organizations are on a journey to transition from DevOps to DevSecOps deployments. This shift brings the demand for new tools, and specialized knowledge. This creates the need for organizations to determine how to support these new requirements. Some organizations have incorporated coaching programs, appointing experts in both security and the development process to guide their development teams through this transition.

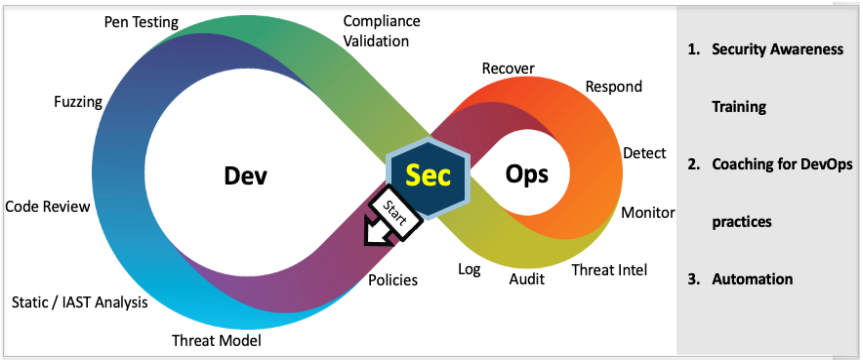

Figure 1 - Shifting Security Left in each phase of SDLC

2.2.5.1. Security awareness training

One aspect of creating a security focused development process is ensuring that all resources contributing to any part of the SDLC are well trained on security best practices and policies, including those in management roles. Ideally this training would be specifically tailored to the role(s) of each participant. Training material could be catered in a tiered level ranging from a base level of understanding all the way to expert. The ideal would be that, after training, participants are able to

demonstrate their knowledge of the security concepts covered before advancing to the next level.

2.2.5.2. Coaching for DevOps practices

With things evolving so fast, it may be hard for development teams to stay on top of emerging security threats and changing security priorities as well as stay focused on improving dev/ops practices to deliver quality products. This need creates an opportunity for security coaching. Security coaches can work with teams to align security practices to the phases in the development lifecycle. These individuals, with an expertise in both security and the software development lifecycle, guide development teams through onboarding new security requirements or shifting processes to incorporate better security practices by assimilating them into their team norms. Coaches can work with teams to understand their workload and constraints, and assist with prioritizing the security work, breaking it down to manageable deliverables.

2.2.5.3. Automation

Another helpful tactic is adding automation around security scans and other security required processes that have made their way into the continuous integration and continuous delivery (CI/CD) pipeline. By introducing automation around these new security requirements, teams are not bogged down with new requirements and things are able to run smoothly. Training the development teams and appointing developers as "security champions" can ensure that as developers built up their skills to handle the fallout of these new processes, the teams could still operate efficiently. [13]

3. Securing Your Customers

The defense strategy against attackers seeking to steal service, customer data, and video content is still evolving. It benefits broadband operators to collaborate both within the industry as well as with external partners to set guiding principles of basic security, communication to customers, and guidance on how to consume their services in secure ways. There are many efforts to secure web interfaces, user logins, and devices by broadband providers. Additionally, the following actions will help to improve the protection for consumers from email threats, account abuses, and device security.

3.1. Identity Protection Capabilities

Implement identity protection capabilities to combat the threats at scale by using AI to support consumers. Comprehensive detection of darknet market ads for account credentials provides the capability to measure the availability of account credentials. This is just an example of one measurement for identifying credentials available for sale in the darknet market. Some additional measures are listed below:

a. External credential spill monitoring and remediation can be built as a basic feature for standard security operations
b. Deep and dark web credential advertisement detection and remediation
c. Robot software agent (BOT) attack prevention at web, application programing interface (API), and mobile authentication interfaces
d. Use internet protocol (IP) information for "geo velocity" and to determine "geo location" to reduce credential theft
e. Implement 2FA or MFA support for consumers and disable less secure authentication methods
f. Detection capabilities using Machine Learning (ML) based tools for credential sharing and compromised accounts
g. Work with law enforcement and other enforcement bodies to identify and disrupt the distribution of unlicensed content

3.2. IoT Device Infection Prevention

In the connected world of customers, internet of things (IoT) devices pose a large threat [14] and have not received full attention. Customers usually do not focus on security measures for devices and forgo more secure devices for their less costly counterparts. On top of this, there is not enough standardization of security control requirements for device vendors. Also, vulnerabilities for these devices do not get addressed regularly. Bringing privacy awareness to device security features as well as how to keep devices up to date with the latest patches is the key to protect individuals from being attacked via their connected devices. Internet providers are offering internet security solutions which block access to compromised or malicious domains and protect customer devices from these threats.

IoT device infections have grown 100% during Covid. [15] This surge in the rate of device infections, directly matches the trajectory of the visibility of the devices on the internet. The cybercriminals probe these devices for security vulnerabilities and exploit them to control the device with unauthorized access, damage it, or penetrate to other devices on the same network. Antivirus software and intrusion detection capabilities are the first layer of security to protect these devices from infections. [16]

IoT is here to stay, and it will continue to grow tremendously, as will the attack surface. The industry demands security leaders to develop a comprehensive IoT lifecycle approach and an IoT security posture to protect and enable IoT devices from both existing and unknown threats. Also, consumer awareness for various precautions to protect the IoT devices is of utmost importance.

3.3. DDoS Attack Mitigation

The exposure of IoT vulnerabilities has dramatically changed the landscape of Distributed Denial of service (DDoS) attacks in recent years. These devices have enough compute power to launch any processes using BOTs and create an attack on other devices. Along with detection measures, effective preventive measures are important to combat the DDoS attacks. Many Threat Intelligence subscription services "Always-on DDoS Protection" are evolving

to help combat these threats and help the customers. [17] [18]. These capabilities include preventive, detective, and mitigation controls which automatically or on-demand mitigate the DDoS attacks.

3.4. Protect Customer Data

In today's data driven customer interactions, businesses rely on large amounts of data being available every second of the day without a blip. The Network Data Loss Prevention (DLP) solutions are relied upon by many organizations, but data breaches happen all the time. Hence there is more to do to protect the data. Privacy initiatives and recent Executive orders provide guidance on some controls around securing data for user identities. They also highlight a need for data-centric tools to build personally identifiable (PI) data inventory, creating data classification policies, performing data discovery, and other initiatives that address data privacy concerns around customer data. To safeguard the data, the use of data encryption and data de-identification practices provide protection but are still evolving. Another key factor in securing data is ensuring that there are strict policies around granting access to and removing access from sensitive data as needed.

3.5. Customer Education

A recent, sophisticated phishing scheme was uncovered in which consumers of unlicensed content were sent an email indicating their free trial was ending and their credit cards were about to be charged. They were directed to a fake website and informed that to cancel their subscription, they must download an Excel file, which contained a ransomware program commonly used by the REvil ransomware group. This is one of the many dangers consumers encounter in their daily lives. It is important to educate consumers of such risks and provide guidance on how to stay safe online.

The Cable and Telecommunications Association for Marketing (CTAM) has seen the need for educating consumers on various security topics and have created a website for sharing information on how to stay safe when streaming content on the internet (streamsafely.com). [19] The dangers of accessing television/streaming content through illegal pirate services and the risks involved in unauthorized password sharing are a few examples of the topics covered on customer education website. As the customer pattern changes and new services are offered, educating customers is essential in keeping the eco-system secure. Developing and sharing tools with industry partners, programmers, studio, and law enforcement, foster partnerships that create better protection for all connected consumers, not just service subscribers.

Figure 2 - Streamsafely.com educational articles

3.6. Industry Alliances required to combat the email Fraud

Customer communications have shifted significantly over the last decade to boost customer service, customer retention and engagement. Email communication is still heavily utilized for notifications or verification of identity during certain events for service changes. Email accounts are one the most sought-after types of credentials because they can be used as a pivot to identity theft. Some email clients on customer devices may be old and vulnerable to attacks due to flaws in email client protocols. An alliance is required between third party email providers to deprecate older email clients and encourage customers to deploy secure new clients.

Below are some actions which can be considered to secure email:

a. Disable unused 3rd party email clients
b. Modernize authentication for 3rd party email clients using oauth
c. Implement email platform anti-abuse capabilities (anti-spam, anti-malware, anti-phishing, anti-viral)

As an abundance of user interfaces are consumed for various user activities, account misuse (knowingly or unknowingly) is extremely high. This demands a defense in depth approach to all attack surfaces. The layering of intelligent defenses has shown a demonstratable impact and is recommended by various organizations. Advanced email authentication attack detection and mitigation development, partnering with vendors and dedicated teams of security professionals managing these platforms, help mature the security of email accounts.

4. Monitor Cyberhealth across your eco-system with CyberScores

The cable industry has been working hard over the last decade on security hygiene, regulatory compliance, and protecting themselves and their consumers from bad actors. Many companies have adopted one or multiple frameworks to evaluate, manage, and ultimately reduce risk over time. Some examples of frameworks that provide guidance on best practices are NIST Cybersecurity Framework, ISO 27000 series, SOC2, FISMA, and the Essential 8 Framework. Using frameworks such as these attest to mitigate 85% of cyber threats [20]. A few common best practices from these frameworks are to implement security controls around the following:

a. Patch Management
b. Application Controls for Workstations and Servers
c. Restrictive Admin Privileges
d. Backups
e. 3rd Party Risk Assessments
f. MFA

Businesses implement a variety of tools for assessing security controls based on framework adoption to better understand, manage, and reduce cybersecurity risk and help protect from various threats. These tools are used to collect metrics from possible sources of risk and present this information in dashboards. As security tools evolve, and new tools are added to the ecosystem, there are challenges around how to continuously measure the effectiveness of the security controls from these various tools and identify aggregated overall company risk.

To combine and analyze data from various security tools and frameworks, a robust risk assessment platform can be utilized to quantify and aggregate the risk and drive meaningful actions for the business.

A few products have emerged with the capability to collect data from various sources and quantify the overall performance of security controls and produce a meaningful cyber risk score dashboard or a Cyber Risk report [21] [22]. Some products also provide compliance assessment based on industry standards and even go beyond to simplify the scores by mapping them to risk ratings [23]. While the maturity of these products is in the early stages, businesses are looking for ways to develop their own centralized security metrics dashboards. According to Gartner, in the future, cybersecurity risk ratings will likely be utilized the same way credit ratings are used when assessing partners for business relationships [24]. The US department of Defense (DOD) now requires supply chain companies to report a cybersecurity maturity model compliance (CMMC) to the DOD if they provide services to them [25].

The enterprise eco-system is usually complex and the risks for each system are evaluated based on the rate of the issues and the severity. A cybersecurity rating platform enables continuous assessment of the tens of security criteria along with thousands of security checks [26]. Companies can either leverage cyber score tools or develop their own. The risks can be evaluated, assigned weightage, and aggregated for contributions to overall cyber risk score based on the company's risk appetite.

Starting small with just a few security controls and combining to one aggregated score may be a good first step toward a single platform. For example, combining the data from vulnerability assessment tools and 3rd party risk assessments into a single dashboard. Once this step is taken, team can be trained to understand the relevance of the combined have a clearer picture on the actions needed to secure their applications all in one place. As the cybersecurity rating program matures, the CyberScores can help drive the various decisions about cybersecurity risk posture from the application level all the way through to the organizational level.

5. Conclusion

The past decade has thrown security into the spotlight. It is no longer overlooked or addressed only after a damaging and expensive incident. Security is now a part of the conversation at every level of business and government. It is no longer bolted on but built into products and services with an expectation from consumers that those we trust are taking every precaution to protect us from the adversaries. Security professionals strive for the right level of protection to keep attackers out of systems and protect customers. Taking a multi-layered and proactive approach has created many successful outcomes. The industry alliances are also key in each sector to uplift the standards for common services and consumer education. The work cannot stop here. As long as there is value to be gained from their efforts, hackers will continue to create challenges. It is up to all of us to keep security part of the conversation, to learn from every attack, and grow our defenses to prevail.

Abbreviations

2FA	Two Factor Authentication
ACL	Access Control List
AI	Artificial Intelligence
AP	Access Point
API	Application Programming Interface
BOT	Robot Software Agent
bps	Bits per Second
CCPA	California passed the California Consumer Privacy Act
CI/CD	Continuous integration/continuous delivery
CMMC	Cybersecurity maturity model certification
CPNI	Customer Proprietary Network Information
CTAM	Cable and Telecommunications Association for Marketing
DOD	Department of Defense
DLP	Data Loss Prevention
FEC	Forward Error Correction
GDPR	General Data Protection Regulation
HD	High Definition
Hz	Hertz
IP	Internet Protocol
ISBE	International Society of Broadband Experts

K	Kelvin
MFA	Multi-Factor Authentication
ML	Machine Learning
NCTA	The Internet & Television Association
OTP	One Time Password
PI	Personally Identifiable
RDP	Remote Desktop Protocol
SCTE	Society of Cable Telecommunications Engineers
SDLC	Software Development Life Cycle
SEIM	Security Event Information Management
SSH	Secure Shell

Bibliography & References

[1] https://www.securelink.com/blog/81-hacking-related-breaches-leverage-compromised-credentials/
[2] "A Taxonomy of Fraud Experienced by Network Service Providers", online: https://www.nctatechnicalpapers.com/Paper/2020/2020-a-taxonomy-of-fraud-experienced-by-network-service-providers
[3] (https://www.investisdigital.com/blog/technology/why-ransomware-attacks-are-rise)
[4] *https://www.appypie.com/how-voice-technology-is-disrupting-different-industries*
[5] *https://www.idtheftcenter.org/voice-fraud-is-on-the-rise/*
[6] *https://www.darkreading.com/cloud/it-takes-an-average-38-days-to-patch-a-vulnerability*
[7] https://www.microsoft.com/en-us/security/business/zero-trust
[8] https://www.nist.gov/blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify
[9] *https://whatis.techtarget.com/feature/History-and-evolution-of-zero-trust-security*
[10] *https://www.drivelock.com/blog/what-ingredients-does-a-zero-trust-model-consist-of*
[11] https://attack.mitre.org/
[12] *https://cheatsheetseries.owasp.org/cheatsheets/Multifactor_Authentication_Cheat_Sheet.html*
[13] *https://securityintelligence.com/posts/how-to-transform-from-devops-to-devsecops/*
[14] *https://www.iotsecurityfoundation.org/the-iot-ransomware-threat-is-more-serious-than-you-think/*
[15] *https://www.securitymagazine.com/articles/93731-infected-iot-device-numbers-grow-100-in-a-year*
[16] *https://www.justice.gov/criminal-ccips/page/file/984001/download*
[17] *https://www.radware.com/solutions/ddos-protection/*
[18] *https://business.comcast.com/enterprise/products-services/cybersecurity-services/ddos-threat-mitigation?CMP=KNC-GOOGLE&utm_source=google&utm_medium=cpc&utm_campaign=ENT_Ethernet_DDoS_BR_E_National&utm_term=comcast%20ddos%20protection-43700049663074668-VQ16-c-VQ6-398589687487-VQ15-&kw=comcast%20ddos%20protection&ad=398589687487&c=ENT_Ethernet_DDoS_BR_E_National&VQ16-c-VQ6-398589687487-e&ds_kid=43700049663074668&gclid=Cj0KCQjw7MGJBhD-ARIsAMZ0eevkouggwHGG5OCIYzmygAnf2Eb5RORp5bTDcasJKzgoGGFL12TLDsAaApsKEALw_wcB&gclsrc=aw.ds*
[19] *https://streamsafely.com/*
[20] *https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model*

[21] *https://support.securityscorecard.com/hc/en-us/articles/360059534531-How-does-SecurityScorecard-implement-the-fair-and-accurate-ratings-principles-*
[22] *https://www.bitsight.com/glossary/cyber-risk-report*
[23] https://www.upguard.com/blog/what-are-security-ratings
[24] https://www.gartner.com/en/documents/3884271/innovation-insight-for-security-rating-services
[25] *https://www.rjo.com/wp-content/uploads/2020/11/What-DODs-Use-Of-Cyber-Scores-May-Mean-For-Contractors.pdf*
[26] *https://csrc.nist.gov/CSRC/media/Presentations/Creating-a-Cybersecurity-Scorecard/images-media/Developing%20a%20Cybersecurity%20Scorecard.pdf*

