



borwood
global technology partner

2023 WHITE PAPER | CYBER SECURITY

Confronting CX Data Security Threats.

INTRODUCTION

Confronting CX Data Security Threats

The annual CxOutsourcers global mindshare event was held in Glasgow, Scotland in May 2023. The event brought numerous leaders together from the customer experience (CX) and business process outsourcing (BPO) industries, with the goal of sharing and gathering knowledge on the latest trends, research, strategies, and best practices.

At the event, a roundtable discussion took place to unpack the importance of cyber and data security in CX. With increasing numbers of cyberattacks on businesses of all sizes, protecting CX data has become paramount. Not only do data threats directly impact customers, but they pose a great risk for the businesses responsible for the data – with the possibility of experiencing immense loss in finances and reputation.

In fact, cyberattacks have increased in both quantity and ‘quality’, with attacks becoming more and more sophisticated. Attackers are targeting businesses through impressive social engineering manipulation tactics and utilizing the latest technological advancements to their advantage.

By effectively safeguarding customer data, businesses can prevent financial losses, preserve brand reputation, ensure operational continuity, and comply with regulations. Establishing a strong and ongoing cybersecurity strategy means that businesses can build trust, provide a seamless customer experience, and establish themselves as reliable partners.

CYBERSECURITY:

The threat landscape

As CX-centric businesses rely increasingly on digital technologies and interconnected systems, they face a rapidly evolving threat landscape. In this section, we will explore the various types of cyber threats that modern contact centers encounter and the potential impact they can have on the organization.

Malware and ransomware attacks

Malware, including ransomware, poses a significant threat to contact centers. Malicious software can infiltrate systems through infected email attachments, compromised websites, or unauthorized downloads. Once inside the network, malware can disrupt operations, steal sensitive customer data, or encrypt files, rendering them inaccessible until a ransom is paid. Such attacks can lead to financial losses, reputational damage, and erosion of customer trust.

In 2020, ransomware attacks increased by 150%, with an average ransom payment of over US\$178,000 – though businesses have experienced demands of between US\$1 million to 2 million.¹

It was noted by a respondent at the CXOutsourcers round table discussion, “Ransomware is one piece of the pie, and its’ got many layers to it.”

Social engineering

Social engineering attacks exploit human psychology to manipulate individuals into divulging confidential information or performing actions that compromise security. Approximately 98% of all cyberattacks utilize social engineering to gain access into networks.² Cybercriminals may pose as customers, colleagues, or IT support personnel, leveraging trust and urgency to manipulate employees. With the advancement of social media and publicly available information, attackers can craft highly targeted and convincing social engineering attacks.

Moreover, phishing is a common form of social engineering, where attackers impersonate legitimate entities to trick employees into revealing passwords or sensitive data. This is often organized through email inboxes, with 96% of social engineering attacks occurring through this path.³

Contact centers are particularly vulnerable to social engineering due to the high volume of customer interactions and the potential for confidential information to be extracted through manipulation.

Distributed denial of service (DDoS) attacks

DDoS attacks aim to overwhelm a contact center’s infrastructure, rendering it inaccessible to legitimate users. Attackers achieve this by flooding the target system with a massive volume of traffic from multiple sources. These attacks have evolved in scale and complexity, with attackers employing botnets, amplification techniques, and multi-vector approaches to increase their effectiveness. Astonishingly, DDoS attacks can disrupt customer service operations, result in service downtime, and lead to significant financial losses.

¹ [Group-IB Report: Ransomware Uncovered 2020/2021](#)

² [PurpleSec 2023 Cyber Security Statistics](#)

³ [2023 Data Breach Investigations Report](#)

A respondent at the roundtable discussion shared that their business had regularly experienced attempted DDoS attacks, noting that “we continuously monitor the traffic, usually getting 100 – 200 visitors per minute and then all of a sudden it would jump to 10,000. And that is a DDoS attack. You need to have DDoS protection.”

Due to the pandemic, the ecommerce industry has experienced a considerable increase in size. This facilitated an enormous surge in DDoS attacks. In fact, in 2020, the annual number of DDoS attacks increased by 154%, with the average attack lasting over 15 hours – and the longest attack lasting almost six days.⁴

Insider threats

Insider threats involve employees or third parties with authorized access to the company’s systems and data. These individuals may intentionally or unintentionally exploit their privileges to disrupt operations and compromise systems. Attackers can steal sensitive information, deploy phishing emails or malware, obtain account credentials, and alter or exfiltrate data.

Often in collaboration with other cyberattack tactics like social engineering, insider threats can be difficult to detect as the attackers often possess legitimate credentials and knowledge of internal processes. According to 2023 research, 74% of organizations are “at least moderately vulnerable” to insider threats, and more than 50% of organizations have experienced an insider threat in the last year.⁵

Third-party risks

Contact centers often rely on third-party vendors or service providers for various functions, such as cloud hosting, software development, or customer data management. However, these partnerships introduce additional cybersecurity risks. If a third-party vendor experiences a security breach, it can potentially expose sensitive customer data or provide attackers with a pathway to infiltrate the contact center’s systems.

This issue was emphasized by a respondent at the roundtable discussion, who mentioned that it is important to “think about all of your vendors, and are all of your vendors protected?”

⁴ [Neustar Security Whitepaper: Cyber Threats & Trends 2020](#)

⁵ [Cybersecurity Insiders 2023 Insider Threat Report](#)

Regulatory compliance and data privacy

Moreover, contact centers are subject to various data protection regulations, such as the General Data Protection Regulation (GDPR) or the Payment Card Industry Data Security Standard (PCI DSS). Failing to comply with these regulations can result in legal consequences, financial penalties, and reputational damage. Cybersecurity breaches that compromise customer data can lead to regulatory violations and severe consequences for the organization.

IMPACT OF CYBER ATTACKS

The consequences of cyberattacks can be devastating for businesses, particularly CX-centric organizations that heavily rely on digital systems and managing sensitive customer data. Executives and decision-makers need to be aware of the alarming facts surrounding cybersecurity to understand the potential impact on their organization. This section highlights key statistics that emphasize the gravity of the situation.

Cost of cybercrime

Cybercrime continues to be a costly problem for businesses worldwide. According to a report by Cybersecurity Ventures, the global cost of cybercrime is projected to reach US\$10.5 trillion annually by 2025, up from US\$3 trillion in 2015.⁶

This substantial increase demonstrates the growing financial impact that organizations face due to cyberattacks. By proactively investing in strong data security, businesses can protect themselves from far heavier costs caused by data breaches.

Rise of ransomware attacks

Ransomware attacks have seen a significant surge in recent years, causing substantial disruptions and financial losses. According to the Federal Bureau of Investigations' (FBI) Internet Crime Complaint Center (IC3), ransomware victims reported over US\$4.4 billion in losses in 2020 alone. This represents a staggering 300% increase in reported losses compared to the previous year.⁷ These attacks often target contact centers and can cripple operations, compromise customer data, and result in reputational damage.

⁶ [Cybersecurity Ventures 2022 Official Cybercrime Report](#)

⁷ [FBI's IC3 Internet Crime Report 2020](#)

Prevalence of phishing attacks

Phishing attacks remain a primary method for cybercriminals to exploit individuals and gain unauthorized access to sensitive information. In 2022, the Anti-Phishing Working Group (APWG) reported a record-breaking number of phishing attacks, with over 4.7 million attacks.⁸ These attacks often target contact center employees who handle customer interactions, putting customer data and the organization at risk.

Expanded attack surface due to remote work

The shift towards remote work in response to the COVID-19 pandemic has expanded the attack surface for cybercriminals. According to statistics collected by GitNux, there has been an 80% increase in email phishing attacks since remote working became a global norm, and 63% of businesses have encountered data breaches caused by employees working remotely.⁹

This expanded attack surface presents new challenges for securing endpoints, ensuring secure remote access, and protecting sensitive customer data.

CHALLENGES IN PROTECTING CONTACT CENTERS AGAINST CYBER THREATS.

Protecting contact centers against cyber threats is a complex task that poses significant challenges for executives and decision-makers. This section outlines the key challenges faced by executives in safeguarding their businesses against cyber threats.

These challenges include limited budgets, system complexity, insider threats, and the rapidly evolving threat landscape. Importantly, potential strategies for addressing these challenges are reviewed in this section.

Limited budgets

One of the primary challenges faced by executives is limited budgets allocated for cybersecurity measures. Contact centers often operate on tight budgets, and allocating sufficient resources for robust cybersecurity practices can be a significant hurdle. Limited budgets may restrict investments in advanced security technologies, regular security assessments, employee training, and hiring skilled cybersecurity professionals.

⁸ [APWG Phishing Activity Trends Reports](#)

⁹ [Remote Work Cybersecurity Statistics and Trends in 2023](#)

The issue of minimal budget being assigned to cybersecurity was raised by one of the roundtable respondents, stating that, "...it never ceases to amaze me how difficult some security teams find it to get budget." they continued that the issue, "is a mixture of poor budget, not taking it seriously, and the people who are dealing with security don't have a loud enough voice high enough in the organization."

Potential strategies

To mitigate these risks, contact center executives can deploy these strategies:

- *Prioritize cybersecurity investments:* Identify critical areas of vulnerability and prioritize investments based on risk assessment.
- *Leverage cost-effective solutions:* Implement cost-effective security solutions and leverage open-source or cloud-based security tools.
- *Seek external funding opportunities:* Explore grants, government funding, or cybersecurity partnerships to supplement the budget.

System complexity

Conversely, contact centers typically have complex IT infrastructures, integrating various systems, applications, and databases. This is further complicated through the mass migration to remote working environments. As such, this complexity makes it challenging to ensure comprehensive security across all layers and components. Legacy systems, third-party integrations, and rapid technology advancements further contribute to system complexity, increasing the potential attack surface and vulnerabilities.

Potential strategies

To address these vulnerabilities, contact center executives can:

- *Conduct regular risk assessments:* Assess the entire IT infrastructure, identify vulnerabilities, and prioritize security enhancements based on risk exposure.
- *Implement in-depth defense layers:* Employ multiple layers of security controls, including firewalls, intrusion detection systems, encryption, and access controls.
- *Modernize and consolidate systems:* Streamline and update the IT infrastructure to reduce complexity, eliminate outdated technologies, and enhance security posture.

A respondent at the roundtable discussion highlighted the importance of conducting regular risk assessments, stating that, "You need to do risk assessments once a year at the very minimum. Have that penetration test. Make sure you have somebody that can do your patch management – anytime you phone."

Insider threats

Insider threats, including employees with authorized access, can pose significant challenges in protecting contact centers against cyber threats. As mentioned, detecting and mitigating insider threats can be complex, as identifying malicious intent or negligent behavior requires constant monitoring and analysis.

Potential strategies

This frequent monitoring and analyses can include:

- *Employee training and awareness:* Educate employees about cybersecurity best practices, the importance of data protection, and the potential consequences of negligent behavior. This training should be ongoing and up to date.
- *Implement access controls:* Limit user privileges based on job roles, implement multi-factor authentication, and regularly review and update access permissions.
- *Establish incident response protocols:* Develop incident response plans that include monitoring and analyzing user activities, implementing behavior analytics, and responding promptly to suspicious activities.

Rapidly evolving threat landscape

The cybersecurity threat landscape is continuously evolving, with attackers employing new tactics, techniques, and tools. Staying ahead of emerging threats requires constant monitoring, threat intelligence analysis, and timely security updates. Executives face the challenge of keeping up with the evolving threat landscape and adapting their security measures accordingly.

Potential strategies

These security measures should include:

- *Outsource cybersecurity needs:* Consider partnering with external cybersecurity experts who can provide specialized knowledge, threat intelligence, and 24/7 monitoring.
- *Continuous training and education:* Encourage employees and IT teams to stay updated on the latest threats and mitigation techniques through regular training sessions, conferences, and industry forums.
- *Engage in information sharing:* Collaborate with industry peers, government agencies, and cybersecurity communities to exchange threat intelligence and stay informed about emerging threats.

REMOTE WORK:

Complications and compliance

Ensuring maximum compliance around security for people working remotely requires a comprehensive approach that addresses both the human factor and the technological aspects. While remote/'gig' working offers flexibility and convenience, it does pose specific challenges for data security. This section details some steps that can be taken to enhance security and mitigate risks in remote working environments.

Technological tools

It is critical for businesses to put measures in place to safeguard sensitive information and support compliance in a decentralized workforce.

The following technological tools and advancements should be used to keep data as secure as possible, and to mitigate the risk of financial, operational, or reputational loss:

- *Secure remote access:* Implement secure remote access technologies such as VPNs or secure remote desktop protocols (RDP) to ensure encrypted connections between remote workers and company networks. This prevents unauthorized access to sensitive data.
- *Endpoint protection:* Deploy endpoint security solutions that include antivirus, anti-malware, and intrusion detection/prevention systems on remote devices. These tools help detect and mitigate potential threats to remote workers' devices.
- *Data encryption:* Implement strong encryption measures for sensitive data stored on remote devices and during transit. This ensures that even if the data is intercepted, it remains unreadable to unauthorized individuals.
- *Regular security updates:* Maintain a rigorous schedule for applying security patches and updates to all remote workers' devices, including operating systems, applications, and security software. This reduces the risk of vulnerabilities being exploited.
- *Data backup and recovery:* Implement robust data backup and recovery mechanisms to protect against data loss or system failures. Remote workers should be educated on the importance of regular data backups and provided with instructions on how to securely store and recover data.
- *Continuous monitoring and auditing:* Implement monitoring and auditing mechanisms to track remote workers' activities, detect potential security incidents, and identify any unauthorized access attempts or unusual behavior.

- *Secure collaboration tools:* Provide remote workers with secure communication and collaboration tools that encrypt data and ensure confidentiality, such as secure messaging platforms or virtual meeting applications with end-to-end encryption.

Preventing human error

Responsible for 95% of cybersecurity breaches, human error is one of the biggest contributors to cybercriminals succeeding in their efforts.¹⁰

A respondent from the roundtable discussion mentioned that, “the biggest vulnerability is people, because it moves from just a dodgy email to social engineering.”

This vulnerability often arises when employees become targets of social engineering tactics or unintentionally make mistakes that expose the organization to risk. As such, these risks can be lessened with the following best practice:

- *Security awareness training:* Provide comprehensive security awareness training to remote workers, covering best practices for data protection, safe browsing, phishing awareness, and secure remote access protocols. Educate them about the importance of maintaining data confidentiality and the potential risks associated with remote work.
- *Strong password practices:* Emphasize the importance of strong and unique passwords for all accounts and encourage the use of password managers. Remote workers should be educated on password hygiene, including regular password updates, avoiding password reuse across multiple accounts, and not storing passwords where they are easy to access by hackers (e.g. Google Docs).
- *Multi-factor authentication (MFA):* Implement MFA across all remote access points to add an extra layer of security. This helps ensure that even if a password is compromised, unauthorized access is prevented unless the second authentication factor is provided. Three-factor authentication has also

¹⁰ [World Economic Forum Global Risks Report 2022](#)

started circulating in recent years as an ever great defense against cybercrime, which often includes facial recognition technology or biometric scanning.¹¹

- *Secure Wi-Fi connections:* Remote workers should be encouraged to connect to secure Wi-Fi networks and avoid using public or unsecured networks, such as those found in restaurants and airports. Encourage the use of virtual private networks (VPNs) to encrypt data transmitted over the internet and provide a secure connection to corporate resources.
- *Device security:* Remote workers should be required to maintain up-to-date antivirus software, firewall protection, and regular software updates on their devices. Additionally, organizations can implement mobile device management (MDM) solutions to enforce security policies and remotely manage and secure employee devices.

On the importance of employee training, a roundtable respondent highlighted that, “95% of your risk can be taken out with just basic proper training parameters and culture changes in your business. 95%. But it needs to be ongoing. Because cyber criminals are constantly getting better. It’s constantly changing.”

Another key aspect of cybersecurity and preventing human error is ensuring that leaders and decision-makers are **creating a culture of security** within the company. By fostering a culture that prioritizes cybersecurity, leaders can build a proactive and resilient environment where employees are equipped with the knowledge and tools to identify, prevent, and respond to cyberthreats effectively. Such a culture promotes a sense of responsibility, accountability, and vigilance among all members of the organization, ensuring that cybersecurity becomes ingrained in every aspect of the business.

Moreover, a strong cybersecurity culture not only protects the company’s assets but also enhances its reputation, instilling trust among customers, partners, and stakeholders. It demonstrates a commitment to safeguarding information, which establishes the organization as a reliable and trustworthy entity in the marketplace. Ultimately, leaders and decision-makers who prioritize cybersecurity culture demonstrate their understanding of the evolving threat landscape and their dedication to mitigating risks, thereby safeguarding their organization’s success and longevity.

Noted by a roundtable respondent, “You need to have a culture within your business and within your customers’ business that tries: ‘We will be a security-first business.’ ...as a leader, you need to lead, to say, ‘we will be conscious, our culture

¹¹ [12th International Conference for Internet Technology and Secured Transactions: Three factor authentication](#)

will be security first, and we'll do everything possible to protect our business and our people.”

Remote working poses unique challenges for data security due to the decentralized nature of work environments and the potential for a diverse range of devices and networks. Organizations should develop clear policies and guidelines specific to remote workers, outlining security requirements, acceptable use of technology, and reporting procedures for security incidents. Regular communication and training on security practices and ongoing monitoring of compliance are essential to mitigate the risks associated with remote work.

CONCLUSION

In the current digital age that is constantly transforming, robust and proactive data security is paramount.

A roundtable respondent highlighting the criticality of data, “...the new value of money is data. Data is going to become that value instead of money. As a business owner, in my opinion, the only way you’re going to realize that is if you start handling your data, treating your data, as if it was money.”

Protecting CX data from cyberthreats is of utmost importance for businesses in today’s digital landscape. Cyberattacks are increasing in sophistication, targeting contact centers through malware, social engineering, DDoS attacks, insider threats, and third-party vulnerabilities.

Failure to safeguard customer data not only leads to financial losses and reputational damage but also regulatory violations. The consequences of cyberattacks can be devastating, with rising costs of cybercrime and the prevalence of ransomware and phishing attacks.

Executives and decision-makers face challenges in protecting contact centers, including limited budgets, system complexity, insider threats, and the rapidly evolving threat landscape. To address these challenges, businesses can prioritize cybersecurity investments, implement cost-effective solutions, conduct risk assessments, and enhance employee training and awareness.

Remote work presents additional complications, requiring secure remote access, endpoint protection, data encryption, regular security updates, and prevention of human error through security awareness training and strong password practices.

Creating a culture of security is crucial for building a proactive and resilient environment. By prioritizing cybersecurity, businesses can protect their assets, enhance their reputation, and build trust among customers and stakeholders.