ONPAGE
SOME MESSAGES CANNOT WAIT

CYBERSECURITY TRENDS TO KNOW

Uncovering Emerging Security Technology, Strategies and Best Practices

www.onpage.com

TABLE OF CONTENTS

03 Introduction

04 Expert Insights on Security Breaches

05 Latest Breaches

06 Why Were Cyberattacks on the Rise?

07 Major Breaches Over the Years

08 Experts on the State of Cybersecurity

09 Emerging Cybersecurity Trends

10 How to Manage Cybersecurity Threats

11 Experts on Recovering From Emerging Breaches

12 Are Firms Spending Enough on Cybersecurity?

13 Conclusions

INTRODUCTION

Cybersecurity continues to evolve through the adoption and implementation of new security systems, strategies and processes. The objective is to prevent malicious parties from breaching critical networks or systems that contain sensitive data.

Cybersecurity teams must collaborate to identify potential security threats and remedy the events using the right resources. It is critical that teams respond to threats promptly to avert the devastating consequences of a cyberattack on business.

This eBook compiles insights from 30 cybersecurity experts across the globe on trends and changes in the industry. Read on to discover the state of cybersecurity.

EXPERT INSIGHTS ON SECURITY BREACHES

COVID forced companies to move their workforce to remote without spending the time or resources to create security best practices … companies need better remote procedures.

Travis Good, MD
CEO and Co-Founder
Haekka

Hackers target the low-hanging fruit: (a) companies that have the most valuable and voluminous data and (b) lax data security protocols. Managed service providers (MSPs)—like the ransomware attack with Kaseya—are good targets because they have the most valuable data.

Matthew Schneider, PhD
Assistant Professor of Data Privacy
Drexel University – LeBow

When hackers find a flaw, they take advantage of it. That is why system flaws can be extremely hazardous. SolarWinds, an American software firm, was the target of a cyberattack in January 2020. After employees disclosed details of the system fault online, cybercrooks exploited a vulnerability in the company's software.

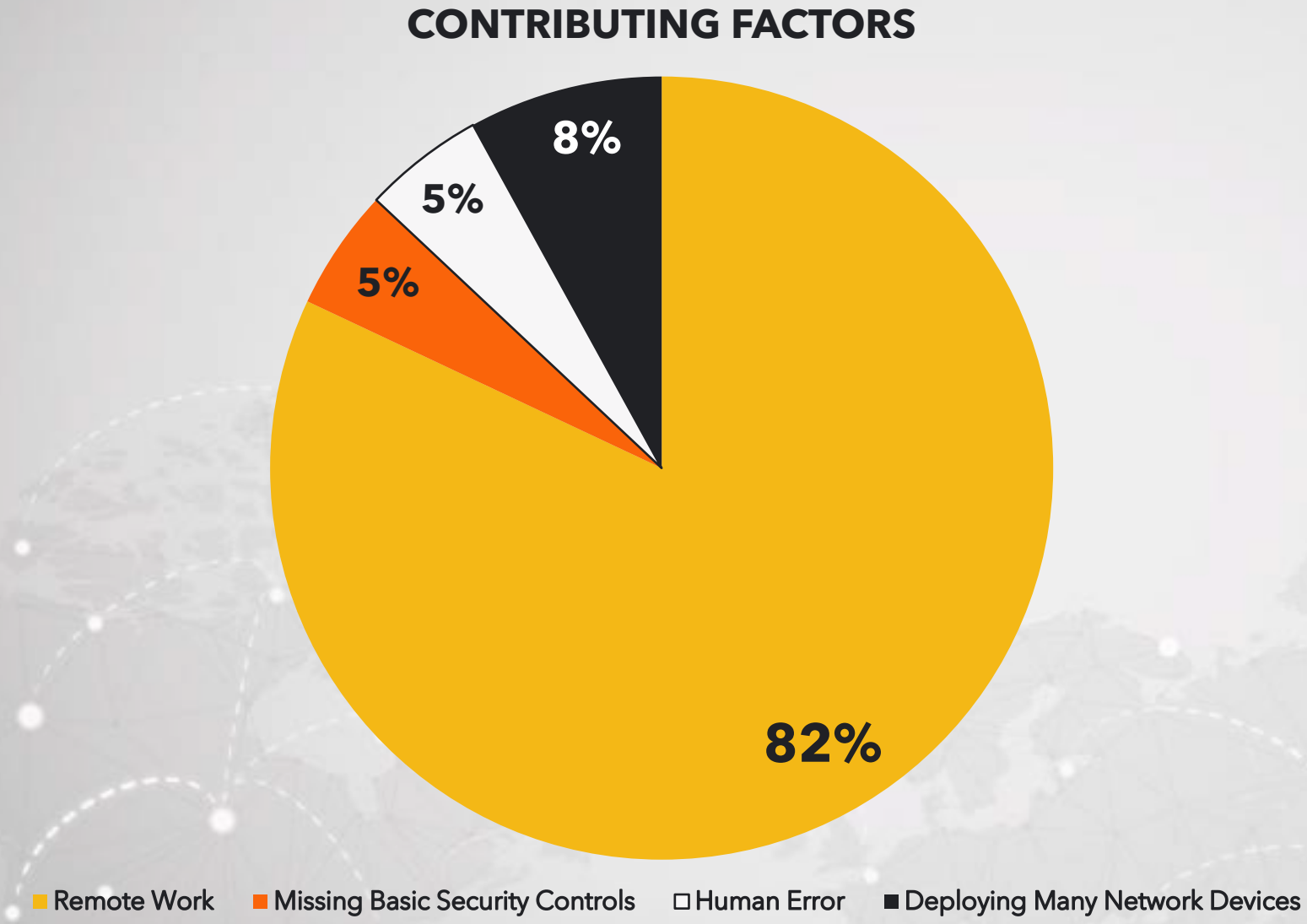
Rameez Usmani
Tech and Security Expert
Code Signing Store

LATEST BREACHES

The previous, unprecedented years consisted of a global health crisis and costly cybersecurity breaches. According to the Ponemon Institute, breaches cost $3.86 million for organizations in recent years.

Key contributors of cyberattacks and breaches include:

1. Unresolved security vulnerabilities
2. Human error and insider threats
3. Malware and ransomware
4. Compromised hardware technology
5. Lack of secure, encrypted internal communications
6. Legacy systems and remote work
7. Sophisticated, new cyberattacks
8. Dedicated hackers



WHY WERE CYBERATTACKS ON THE RISE?

A sample size of 30 cybersecurity experts provided insights on the contributing factors of recent breaches.

According to 82 percent of survey respondents, the key contributor to cybersecurity breaches was remote work. Remote work displaced personnel during the COVID-19 outbreak, and new systems were deployed without proper security protocols to support this "new normal." New IT vulnerabilities were caused by work-from-home requirements.

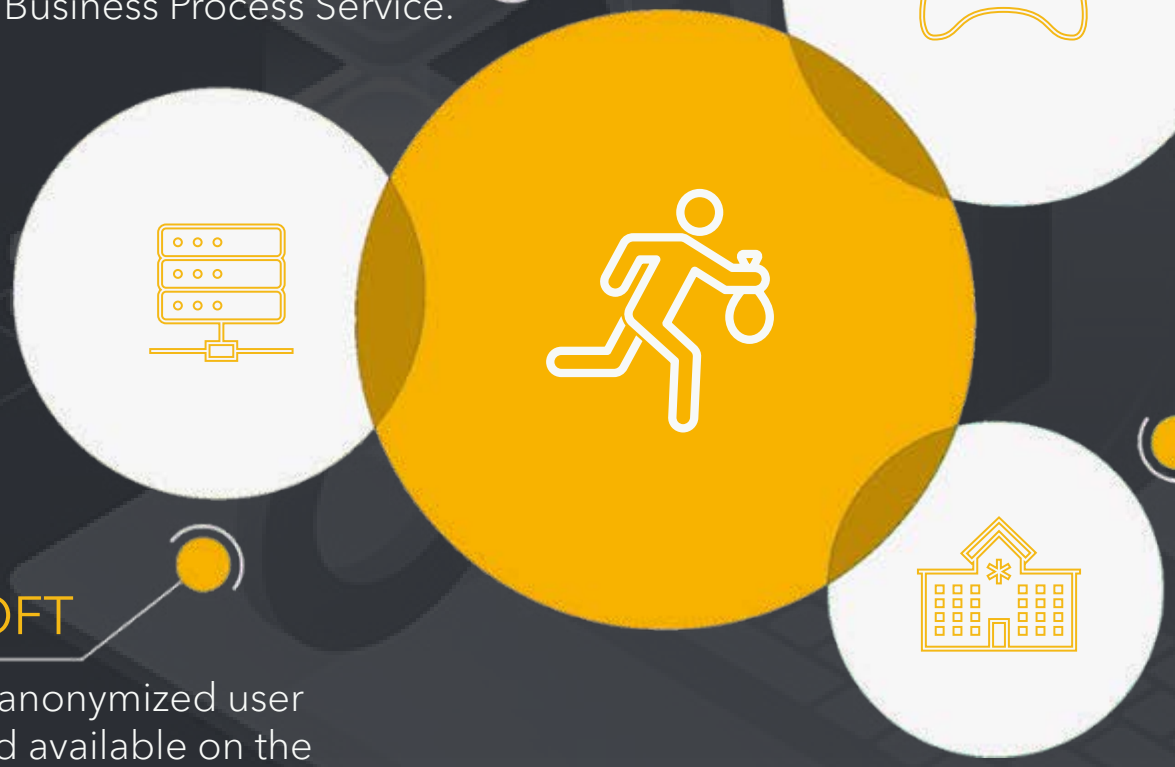
MAJOR BREACHES OVER THE YEARS

GENERAL ELECTRIC

Unauthorized party accessed sensitive worker information due to security failures with supplier Canon Business Process Service.

NINTENDO

160,000 users impacted by a mass account hijacking caused by the Nintendo Network ID (NNID) legacy login system.



DUESSELDORF U. HOSPITAL

Patient dies after being diverted to a nearby hospital after Duesseldorf suffered a ransomware attack.

MICROSOFT

Five servers used to store anonymized user analytics were exposed and available on the Internet without protection.

Source: https://www.zdnet.com/article/the-biggest-hacks-data-breaches-of-2020/

EXPERTS ON THE STATE OF CYBERSECURITY

> Threat actors [operate] like businesses—ransomware is a multibillion-dollar industry—and it's on the rise in every sector … not just because of data-rich personally identifiable information (PII), but because … actors know that most companies are ill equipped to defend against it.

Craig Goodwin
Co-Founder and Chief Product & Strategy Officer
Cyvatar

> Cybersecurity has become much more about data theft and less about machines and systems engineering … privacy-preserving cryptography and distributed ledger [tech] offer zero-trust resolutions to data privacy.

Andrew Weed
Director of Systems Architecture & Cybersecurity
Mind Bank Ai

> [There is] IT/OT convergence, a heightened focus on firmware and hardware security, and an abandonment of perimeter-based security strategies in favor of a Zero Trust approach.

Yanir Laubshtein
VP of Cybersecurity & Industry
NanoLock Security

> Ransomware has surged, becoming the exploit of choice … bad actors have become increasingly sophisticated, in both their technical expertise … [and] business acumen. Some organizations … have call centers and help desks to facilitate ransomware payments.

Mark Kirstein
VP of Customer Success
Cosant Cyber Security

EMERGING CYBERSECURITY TRENDS

Based on the responses from 30 cybersecurity experts, organizations in all industries should be aware of these five emerging trends.

Five emerging cybersecurity trends include:

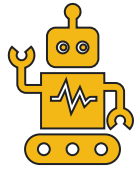
1. Zero Trust security model
2. Rise of new AI/ML-based systems
3. Fixing remote work vulnerabilities
4. New ransomware obstacles
5. Extended detection and response (XDR)

1 Zero Trust Security

Organizations must not automatically trust anyone or any device. Everyone and everything must be authorized before receiving access to the firm's network.

2 New AI/ML

AI, such as generative adversarial networks (GANs), can simulate hackers' actions and allow businesses to adjust their defenses automatically.



3 Fixing Remote Work

Firms are prioritizing better remote procedures, tools to monitor remote workflows, and effective training on remote workforce security.

4 Ransomware Obstacles

Ransomware-as-a-service (RaaS) allows even the most inexperienced actors to launch ransomware. These unlawful services are readily available on the dark web.

5 XDR

XDR collects and automatically correlates data from email, endpoints, servers, cloud workloads and networks, to detect threats and enable security analysts to respond to them faster.

HOW TO MANAGE EMERGING CYBERSECURITY THREATS

CASB + ALERTING

Cloud access security broker (CASB) integrates with incident alerting tools to immediately notify security teams of company policy violations. Improve incident response time whenever security anomalies are detected.

XDR

Provide specific recommendations to security analysts to further investigate an incident through queries. XDR suggests effective countermeasures to eradicate detected security threats.

SECURITY TRAINING

Organizations must train employees on IRP protocols and proper security techniques. Security awareness training ensures that sensitive data is not intercepted during remote work. Train staff to eliminate human error.

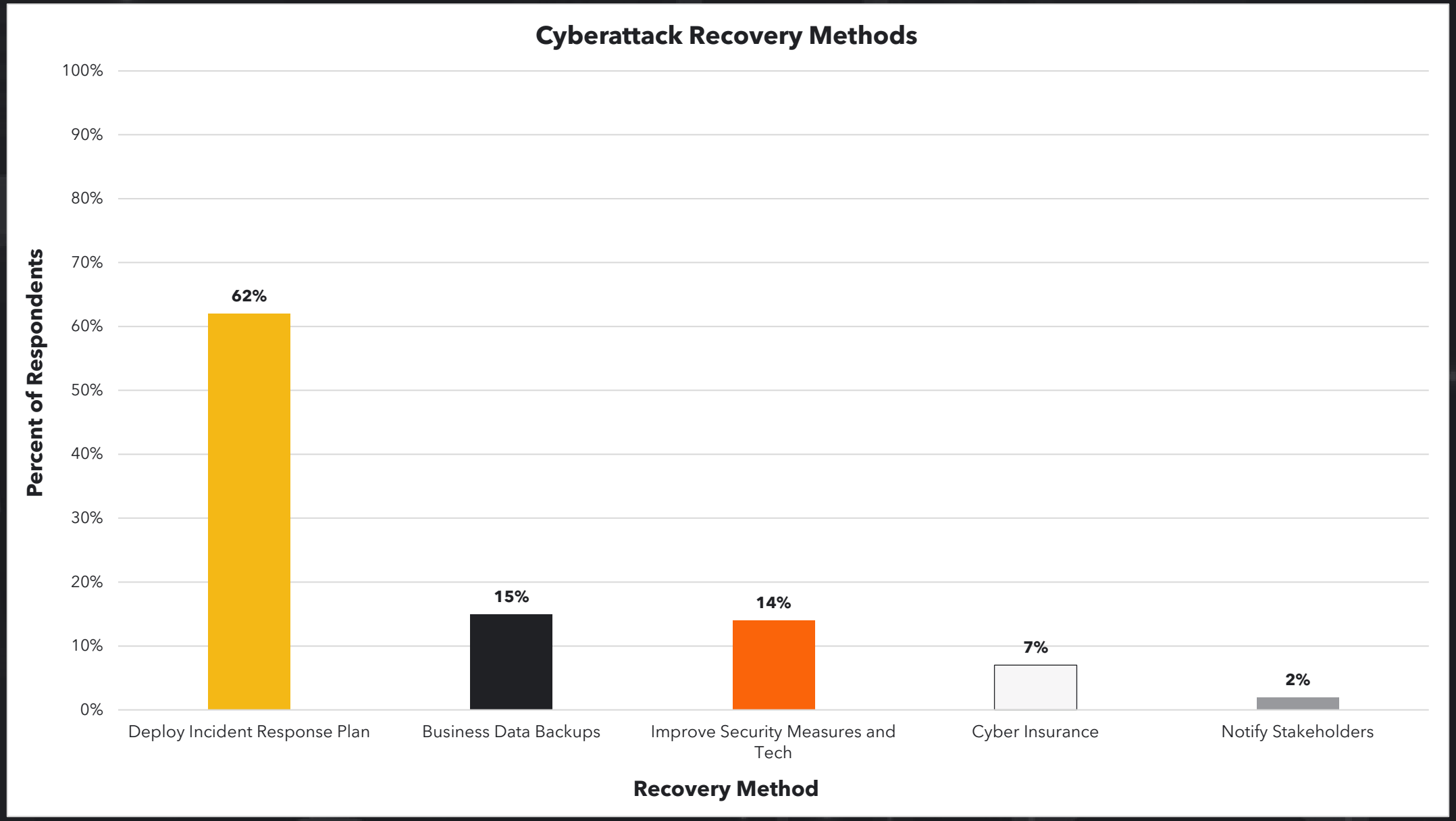
INCIDENT PLANS

An incident response plan (IRP) is a documented method for detecting, evaluating and eliminating threats to systems. IRP steps include preparation, detection, containment, eradication, recovery and refinement.

COMMUNICATE

Cybersecurity teams require secure, critical alerting and messaging applications to communicate with colleagues during cyberattacks. Keep personnel updated and ensure they know who is tasked to manage the security event.

EXPERTS ON RECOVERING FROM EMERGING BREACHES



ARE FIRMS SPENDING ENOUGH ON CYBERSECURITY?

Organizations can determine whether they are investing enough on information security systems and controls by:

1. Conducting risk assessments
2. Making ROI-based decisions on prioritization and investment
3. Calculating the cost of a breach on business and brand reputation
4. Using CIS Critical Security Controls (CSC) to identify vulnerabilities and close the gaps based on priorities
5. Hiring professionals that specialize in gap analysis and incident response

CONCLUSIONS

1. Teams must prioritize security threat prevention before potential attacks occur and cause costly, catastrophic damages for an organization. Firms must focus on threat prevention before remediation.

2. Organizations must build effective, robust incident response plans (IRPs), to mitigate the impact of cyberattacks and immediately bring business operations back to normal.

3. Improving cybersecurity controls and measures is an iterative process. Organizations must constantly conduct risk assessments and identify significant security vulnerabilities. Adopting advanced, secure technology helps close security gaps.

ABOUT ONPAGE

OnPage's award-winning incident alert management system for IT, MSP and healthcare professionals provides the industry's only ALERT-UNTIL-READ notification capabilities, ensuring that critical messages are never missed. OnPage enables organizations to get the most out of their digital investments, so that sensors, monitoring systems, and people have a reliable way to escalate urgent notifications to the right person immediately.

OnPage's escalation, redundancy, and scheduling features make the system infinitely more reliable and secure than emails, text messages and phone calls. OnPage shrinks resolution time by automating the notification process, reducing human errors and prioritizing critical messages to ensure fast response times.

Whether to minimize IT infrastructure downtime or to reduce the response time of healthcare providers in life and death situations, organizations trust OnPage for all their secure, HIPAA-compliant, critical notification needs.

CONTACT US

For more information, visit www.onpage.com or contact the company at sales@onpagecorp.com or at (781) 916-0040.

© OnPage Corporation