convergent

Actionable Insights into Securing Innovative and Collaborative Environments

Chris Johnson
President & Chief Executive Officer

Janice Pearson
Vice President, Global Content Protection

Matt Lucas' impersonation of Boris Jo

convergent

Current state of recovery

https://news.sky.com/story/coronavirus-matt-lucas-video-mocking-boris-johnsons-speech-to-the-nation-goes-viral-11986438

convergent

Ongoing response

Made changes to current infrastructure

Adopted remote working technologies or implemented physical workflows

Integrating collaboration tools and streaming technologies

convergent

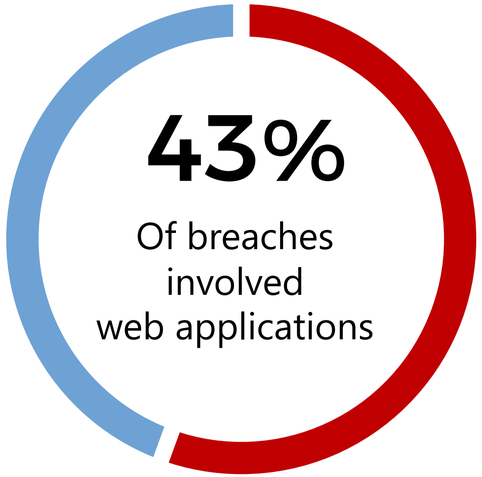
Key trends

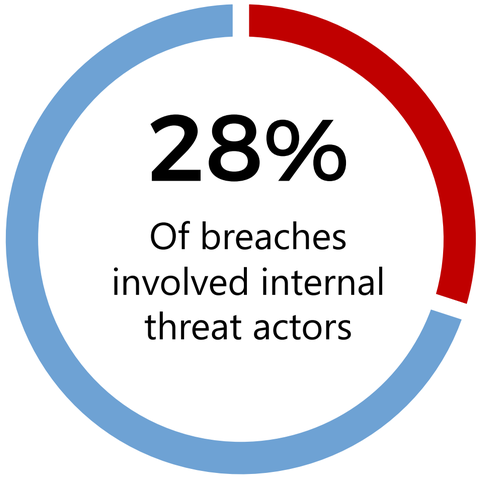
In a Deloitte study, "Automation was the top transformation action arising from the COVID-19 crisis. Globally and across all regions, roughly two of three companies expect to pursue automation."

1. Organizations are reducing their real estate footprint
2. Organizations are redesigning their supply chains
3. New cloud-based workflows are creating opportunities for scale and efficiency by using automation, machine learning, and integration capabilities
4. Increase in streaming technologies and SaaS applications
5. Increased use of digital channels for pre-sale, sale, and post-sale activities

convergent

Verizon breach data

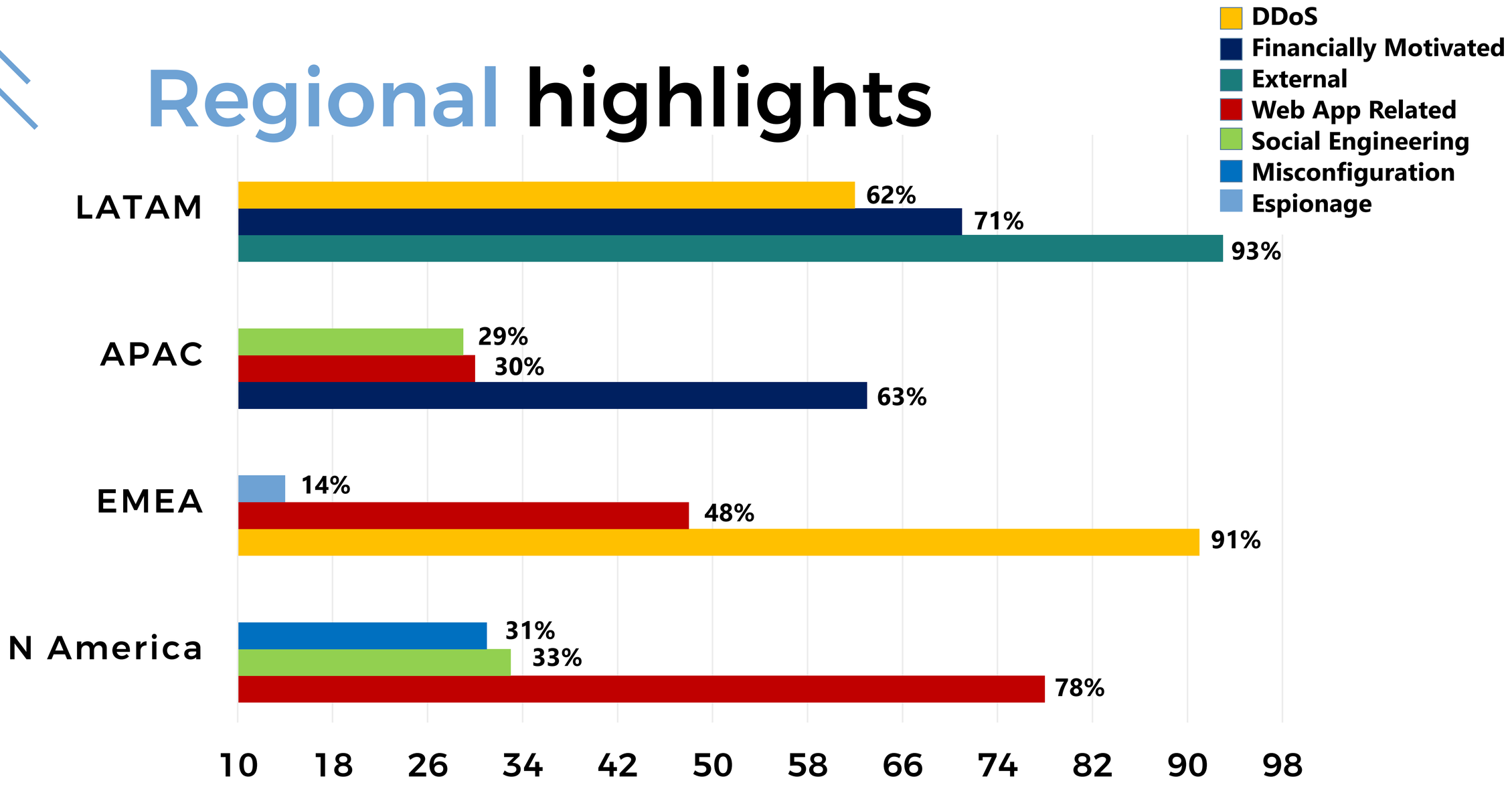




Source: 2020 Verizon Data Breach Investigations Report, which analyzed 3,950 breaches in the United States

convergent

Regional highlights



Source: 2020 Verizon Data Breach Investigations Report

convergent

Key challenges

1. Shared responsibility model
2. Lack of talent
3. Cyber attacks
4. Misconfiguration errors

convergent

Securing applications

convergent

Existing security vulnerabilities now more relevant

1. Improper VPN Access Configuration on a larger scale
2. Lack of logged VPN access to content by administrators – but now on a larger scale
3. Use of personal computers that are not maintained or monitored by IT
4. Personnel working on content from Wi-Fi networks not protected by a software/ hardware firewall
5. Work traffic not segregated from other home devices or IoT solutions

convergent

Security recommendations

1

THINK BEYOND THE PERIMETER

Network monitoring, proxies, multi-factor authentication, and mobile device management

2

VULNERABILITY MANAGEMENT

Continuous monitoring, configuration and patch management, and endpoint protection software

3

LEAST PRIVILEGE

Restrict users, accounts, devices, and computing processes and monitor access

4

WEB BROWSER PROTECTION

Isolated browser or secure gateway technologies to prevent malware and executables

5

EMAIL PROTECTION

Use Password managers, encryption, and egress protection software to prevent breaches

6

SECURITY AWARENESS TRAINING

Train users on phishing, malware, and social engineering attacks and how to avoid them

convergent

Industry assessment observations

250 Assessments conducted March – October 2020

1. Vendors at widely varying levels of maturity
2. Industry standards and best practices require revision and updating
3. Some industry organizations and studios are producing independent security

convergent

More information about our services

info@convergentrisks.com

www.convergentrisks.com

convergent

1

Security Assessments

- Cloud Security
- SaaS Applications
- Service Providers
- Site Security
- TPN

2

Security Consulting

- Design Reviews
- Cloud Migration
- Pre-Assessments
- Privacy Compliance
- SOC2 Preparation

3

Vulnerability Assessments

- Cloud Configuration
- Code Reviews
- Infrastructure Pen Tests
- Vulnerability Scanning
- Web App Pen Tests