Cloud 9 Advisers

Strategic Partners
Technology Experts

Cybersecurity

Technologies

Risk & Security Assessments
Compliance Readiness & Management
Penetration Testing & Vulnerability Assessments
Security Awareness Training & Simulators
Incident Response, Containment, Remediation
Identity Access Management (IAM)
Endpoint Detection and Response (EDR)
Secure Access Service Edge (SASE)
Zero-Trust Network Access (ZTNA)
Secure Web Gateway (SWG)
Software Defined Perimeter (SDP)
Cloud & On-prem Next-Gen Firewall (NGFW)
Disaster Recovery/DRaaS
Security Event Incident Management (SEIM)

Our Leading Suppliers

at&t
CenturyLink
verizon
Trustwave
IGI Solve. Simplify. Secure
HTG 360
RISK SENSE
FORTINET
THRIVE Your Partner for Technology Success
IMPERVA
OMNINET
nitel
Quest TECHNOLOGY MANAGEMENT
ALLGRESS
CATO NETWORKS

With help using our proprietary IT decision-making platform, we help companies make smart IT investments and reduce IT spending by sourcing the right solutions from the right vendors. Whether you're seeking the best new solutions or need assistance with a project outside your wheelhouse, we have the expertise to help. We work with you to identify, research, evaluate, and compare all the solutions and vendors; eliminating months of labor doing it alone.

www.Cloud9Advisers.com
202-996-0757
Consulting@Cloud9Advisers.com

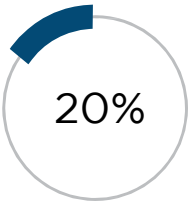
14 Business Impacts of a Cyber Attack

ABOVE the surface	• Technical Investigation • Customer breach notification • Regulatory compliance • Attorney fees and litigation	• Post-breach customer protection • Public relations • New security and IT requirements
BELOW the surface	• Insurance premium increases • Increased cost to raise debt • Impact of operational disruption or destruction	• Value of lost contract revenue • Devaluation of trade name • Loss of intellectual property • Loss of customer relationships

Source: Deloitte & Touche LLP

Over 70% of organizations report having been compromised by a successful cyberattack in the past 12 months

Source: Cyberthreat Defense Report North America & Europe



Only 20% of IT professionals are confident their organizations have made adequate investments in educating users on how to avoid phishing attacks.

Source: Cyberthreat Defense Report North America & Europe

Direct cost

The direct expense outlay to accomplish a given activity, such as engaging forensic experts, outsourcing hotline support and providing free credit monitoring subscriptions and discounts for future products and services.

Indirect cost

The amount of time, effort, and other organizational resources spent in the aftermath of a breach, such as in-house investigations and communications. This category also includes the extrapolated value of customer loss resulting from turnover.

www.Cloud9Advisers.com 202-996-0757 Consulting@Cloud9Advisers.com