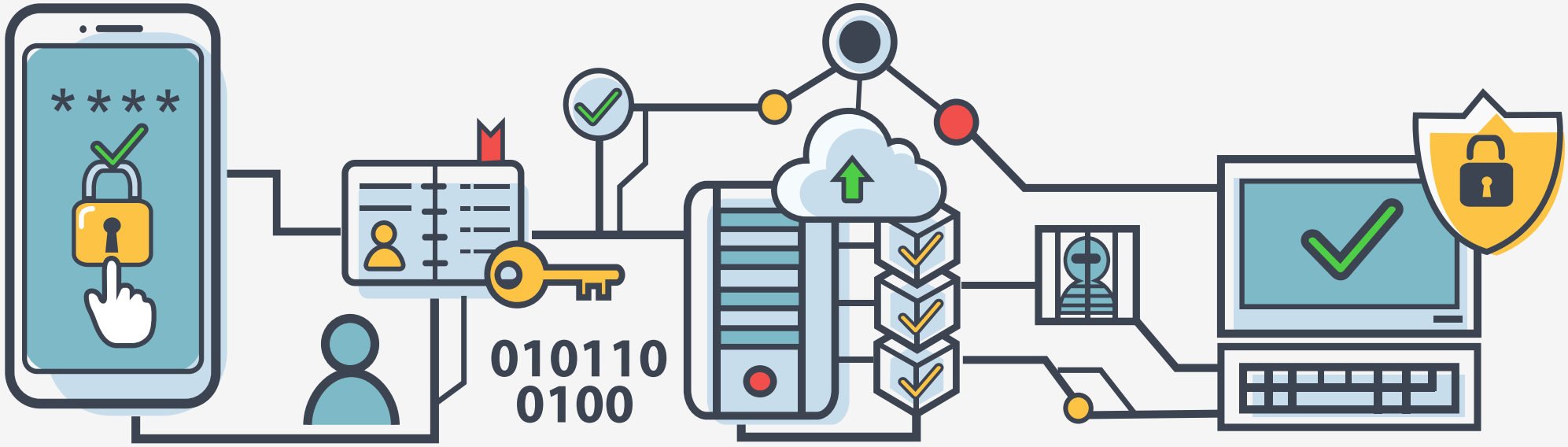
2020
State of Cybersecurity Report



NetGain TECHNOLOGIES

NetGainIT.com/blog

About the Report

The 2020 State of I.T. Services Executive Report is based on an annual survey, conducted by Research Corp., in January and February of 2020.

The report examines usage, approach, and preferences for I.T. services and products, as well as common goals and practices for engagement with I.T. services providers.

RESEARCH METHODOLOGY

Independent databases of top CXOs and I.T. leaders were invited to participate in a web survey conducted by Research Corp., via Survey Monkey.

The 2020 report data comprises responses from 108 organizations, across industries and with <10 to 1000+ employees.

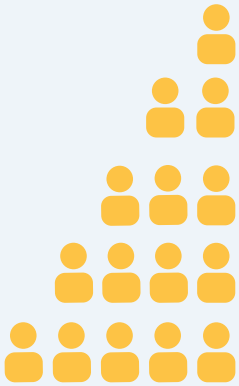
ABOUT NETGAIN TECHNOLOGIES

Since 1984, NetGain Technologies has been a leading provider of I.T. services and solutions. Our managed I.T. services are ranked among the best in the world by Channel Futures and CRN. With a multi-state regional footprint, a three-decade pedigree, over 300 technical certifications and partnerships with vendors such as HPE, Cisco, and Microsoft, we've helped thousands of unique clients thrive by leveraging our best-in-class services and solutions.

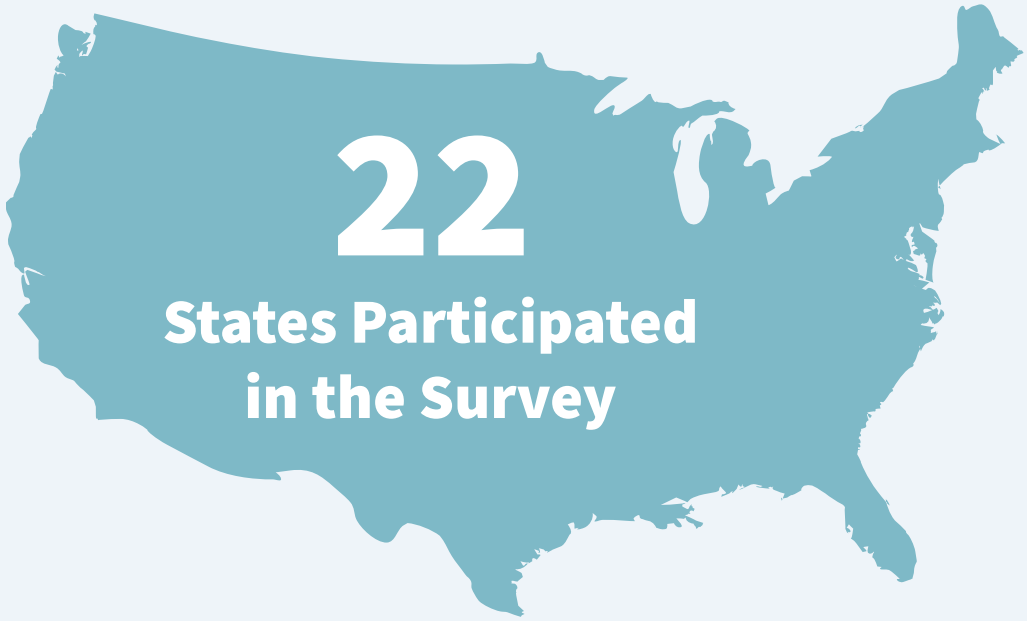
Table of Contents

Survey Respondent Demographics

Number of Employees



35% 1-50
17% 51-100
38% 101-500
8% 501-999
2% 1000+



Size of I.T. Team

26% 1 Person
43% 2-5 People
10% 11-25 People
2% 26-50 People
7% 51+ People

The Ever-Changing Cyber Threat Landscape

81%

of those surveyed said I.T. Security is one of their **top 3 priorities.**

Today's Threat Landscape - Vectors of Concern

Ransomware/Malware via Email

Ransomware/Malware via Web Browsing

Human Error in Securing Systems

Front Door Attack via Firewall

Mobile Device Compromise

Cloud Systems Compromise

Unauthorized Software on Desktops

Physical Theft

Highest Proportion of Organzations Concerned

Lowest Proportion of Organzations Concerned

I.T. Security Management

Security Leaders

59% of Organizations do not have a Chief Security Officer

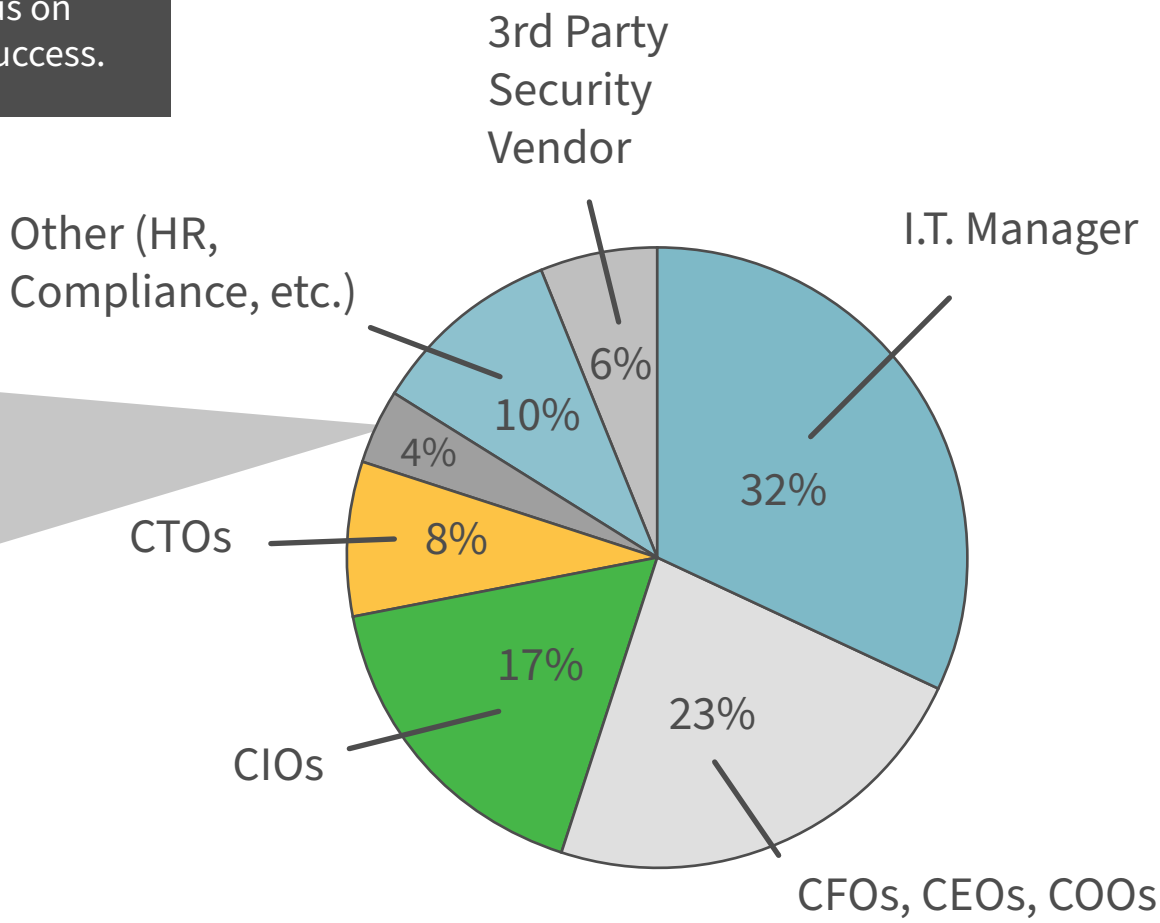
and only **2%** are currently evaulating hiring a CSO.

Corporate security is a specialized and complex area of I.T. services. As the security threat landscape is a living, fire-breathing beast, so too is an organization's strategic security plan. Therefore, a C-level security officer is a valuable and important asset on the leadership team. If a CSO is not employed, the task of security may fall on another indiviual within the organization who does not have the bandwidth or expertise to dedicate to the role, therefore putting the organization at risk.

I.T. Security Management
Non-CSO Security Leaders

While a full-time CSO is optimal, an outsourced security vendor can be an extremely cost-effective alternative to employing a full-time CSO for organizations who either do not have the budget for another C-level executive or, who prefer to trust their security to a team of security experts—freeing the executive team to devote their focus on core business initiatives to drive growth and success.

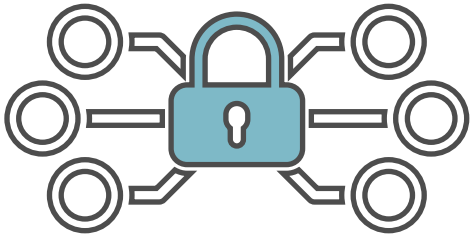
Notice only **4%** of organizations have a CSO managing their security.



Avoid Becoming A Statistic

I.T. Security Planning

I.T. Security Planning
Network Security Policy

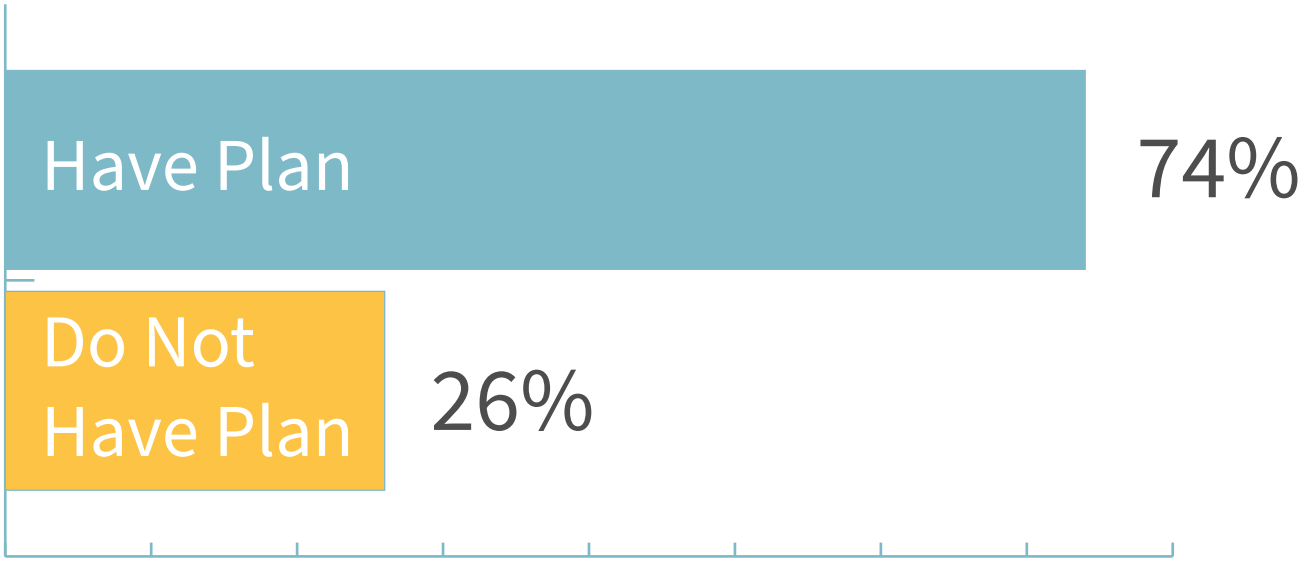


A Network Security Policy documents rules for device access, explains how policies are enforced and covers the basics of your security environment. Every organization should have one.

I.T. Security Planning
Security Breach Plan

A security breach plan documents standard operating procedure (SOP) for response to security incidents and breaches. The plan provides a well-defined and organized approach for handling actual or potential threats to an organization's business operations. The plan is a durable, living document that should be regularly audited and updated, and regular simulations should be conducted to assure the plan works effectively across the company.

Organizations with a Security Breach Plan



I.T. Security Planning

Disaster Recovery & Business Continuity

In today's world, natural disasters, as well as the increasing range of security threats can negatively impact or entirely shut down a business. Having both a Disaster Recovery and Business Continuity is essential.

Both Plans In Place
61%

Disaster Recovery Only
8%

Evaluating
13%

No Plan
10%

Business Continuity Only
7%

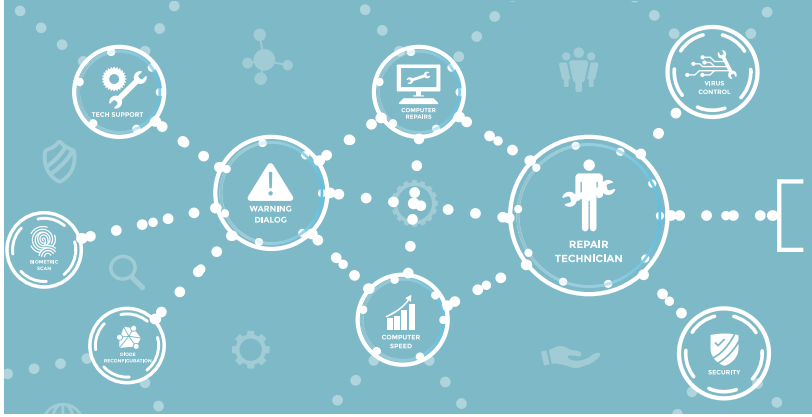
Summary

81% of those surveyed had I.T. Security as one of their top three priorities.

The number one vector of concern for organizations is ransomware/malware via email.

More than half of organizations surveyed do not have a chief security officer.

23% of organizations still do not have a Business Continuity or Disaster recovery plan.



Conclusion

Cybercriminals are taking every opportunity to exploit corporate security vulnerabilities. Every organization must be prepared to handle a security breach.

Organizations are aware, some painfully so, of the many threats to their operational security and most have implemented protection measures. The challenge, to maintain focus on this particular aspect of I.T. and maintain up-to-the-minute knowledge and fluency with evolving technology, is difficult to manage among all the other pressing business tasks.

This is why organizations are increasingly engaging external I.T. services partners who have specialized security planning and implementation expertise to provide virtual chief security officers (VCSO) and security services.

NetGain
TECHNOLOGIES

Have questions about this report, or want to further discuss strengthening your I.T. Security?

Contact NetGain Today!

SMART@NetGainIT.com | NetGainIT.com

844-777-6278

Visit **NetGainIT.com/blog** to find resources on many other I.T. topics on our blog!