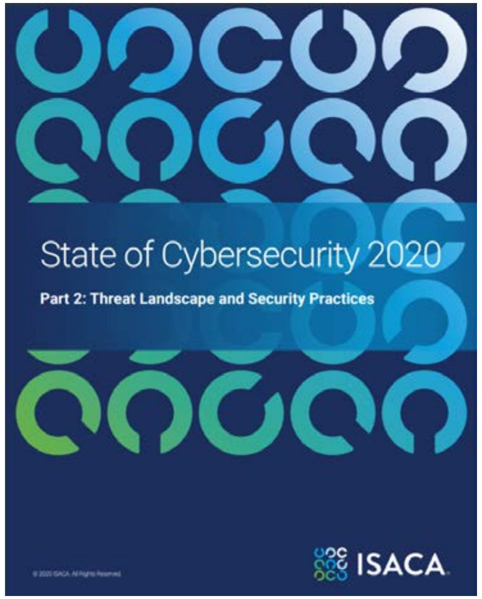
Security Governance: from protection and compliance to business value and confidence

Andrey Drozdov, CISA, CISM, CGEIT, CDPSE, COBIT 2019
ISACA Moscow Chapter, First Vice-President

January 2021

ISACA
Moscow Chapter

Key Sources Used


State of Cybersecurity 2020

Part 2: Threat Landscape and Security Practices

ISACA

© 2020 ISACA. All Rights Reserved

ISACA

A Global Look at Privacy 2020: Trends in Privacy Practices

© 2020 ISACA. All Rights Reserved

Gartner Top 9 Security and Risk Trends for 2020

Security

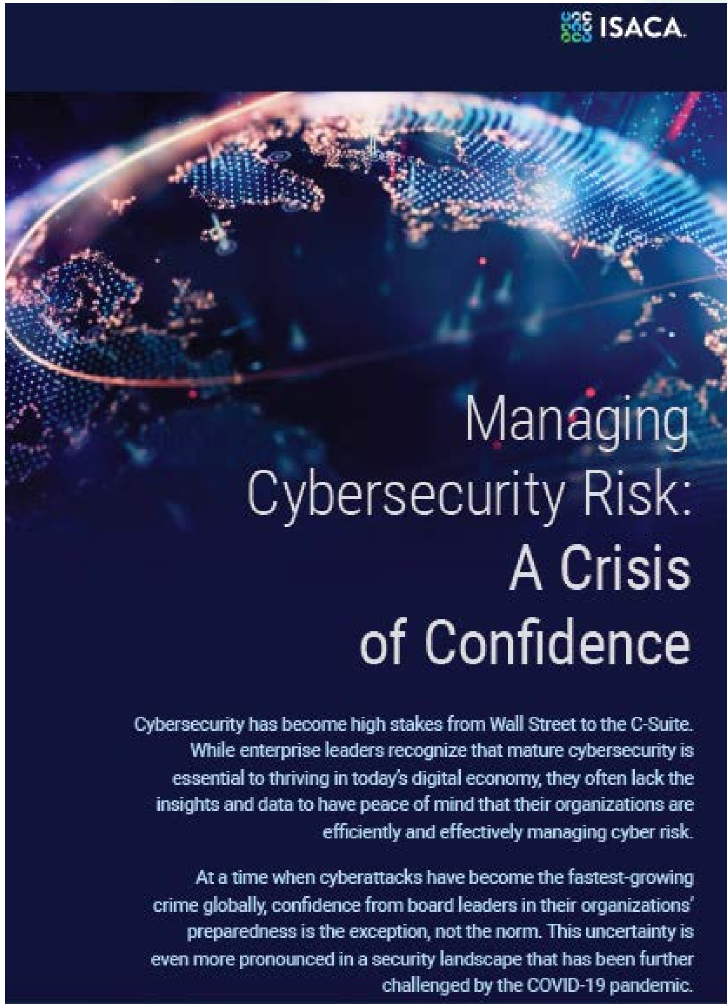
CACS | CSX CYBERSECURITY NEXUS

An ISACA® 2019 European Conference

GTACS 2020

GOVERNANCE · TECHNOLOGY AUDIT · CONTROL · SECURITY

Cyber Resilience to Confidence


ISACA

Managing Cybersecurity Risk: A Crisis of Confidence

Cybersecurity has become high stakes from Wall Street to the C-Suite. While enterprise leaders recognize that mature cybersecurity is essential to thriving in today's digital economy, they often lack the insights and data to have peace of mind that their organizations are efficiently and effectively managing cyber risk.

At a time when cyberattacks have become the fastest-growing crime globally, confidence from board leaders in their organizations' preparedness is the exception, not the norm. This uncertainty is even more pronounced in a security landscape that has been further challenged by the COVID-19 pandemic.

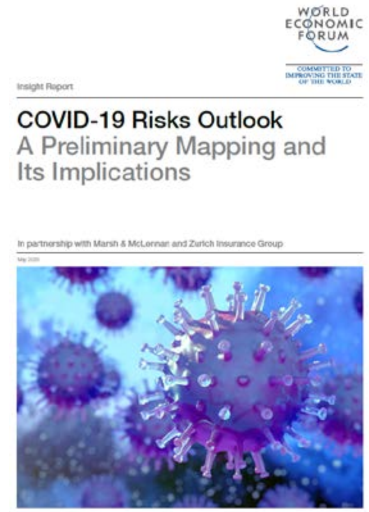
ISACA

protiviti

Face the Future with Confidence

IT Audit's Perspectives on the Top Technology Risks for 2021

Cybersecurity, privacy, data and resilience dominate the top technology challenges for organizations, according to the annual ISACA/Protiviti global survey of IT audit leaders and professionals


WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Insight Report

COVID-19 Risks Outlook

A Preliminary Mapping and Its Implications

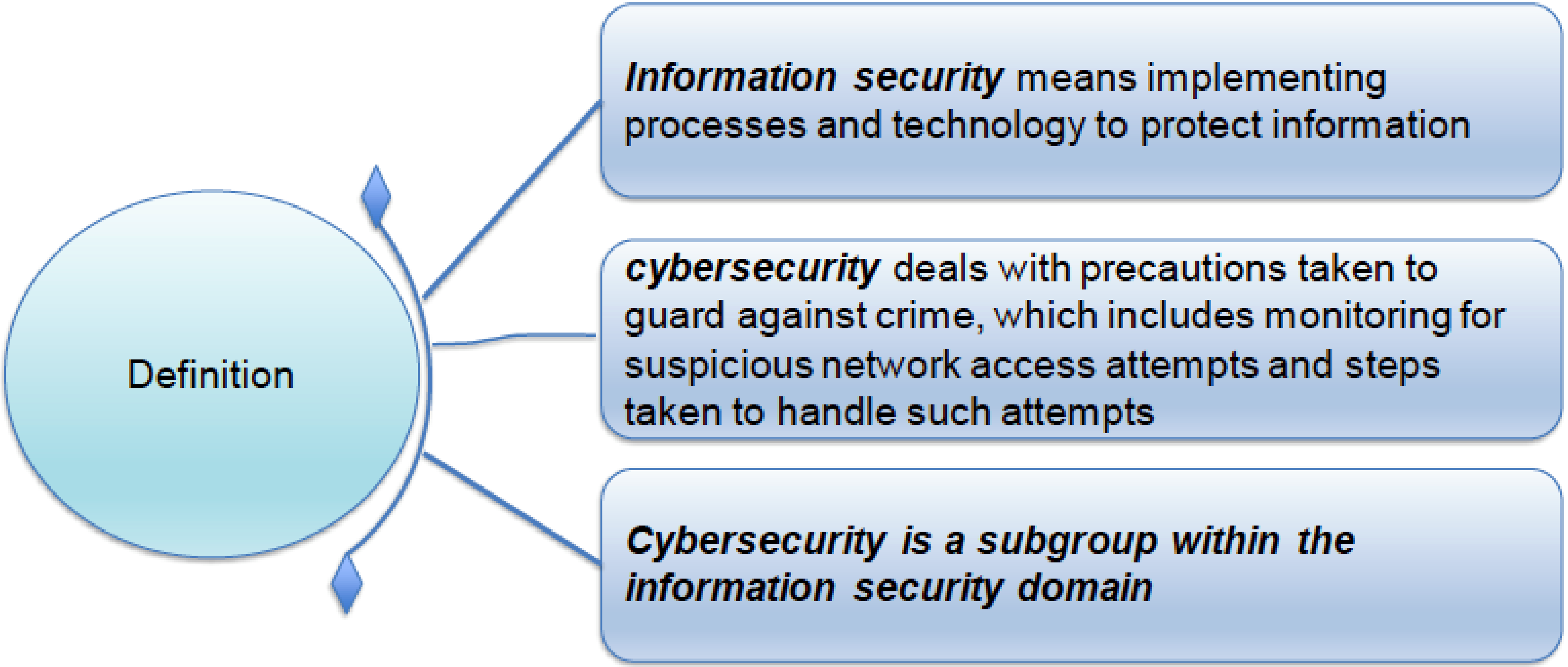
In partnership with Marsh & McLennan and Zurich Insurance Group

May 2020

ISACA

Moscow Chapter

Information Security vs Cyber Security

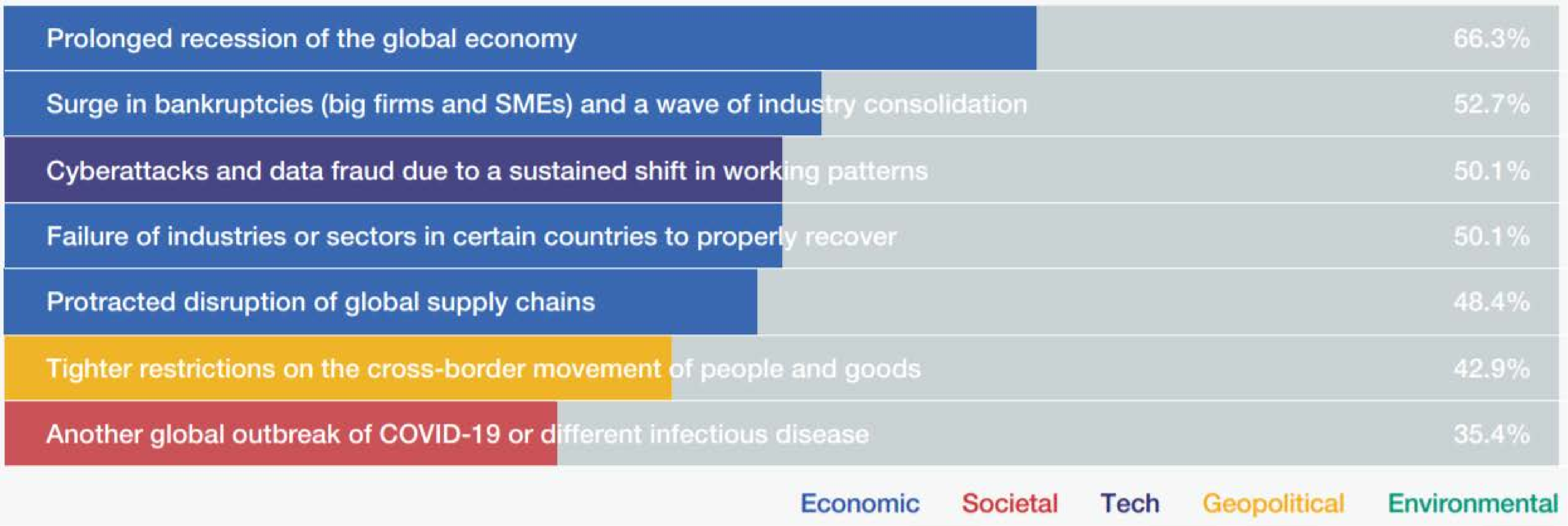


Information security means implementing processes and technology to protect information

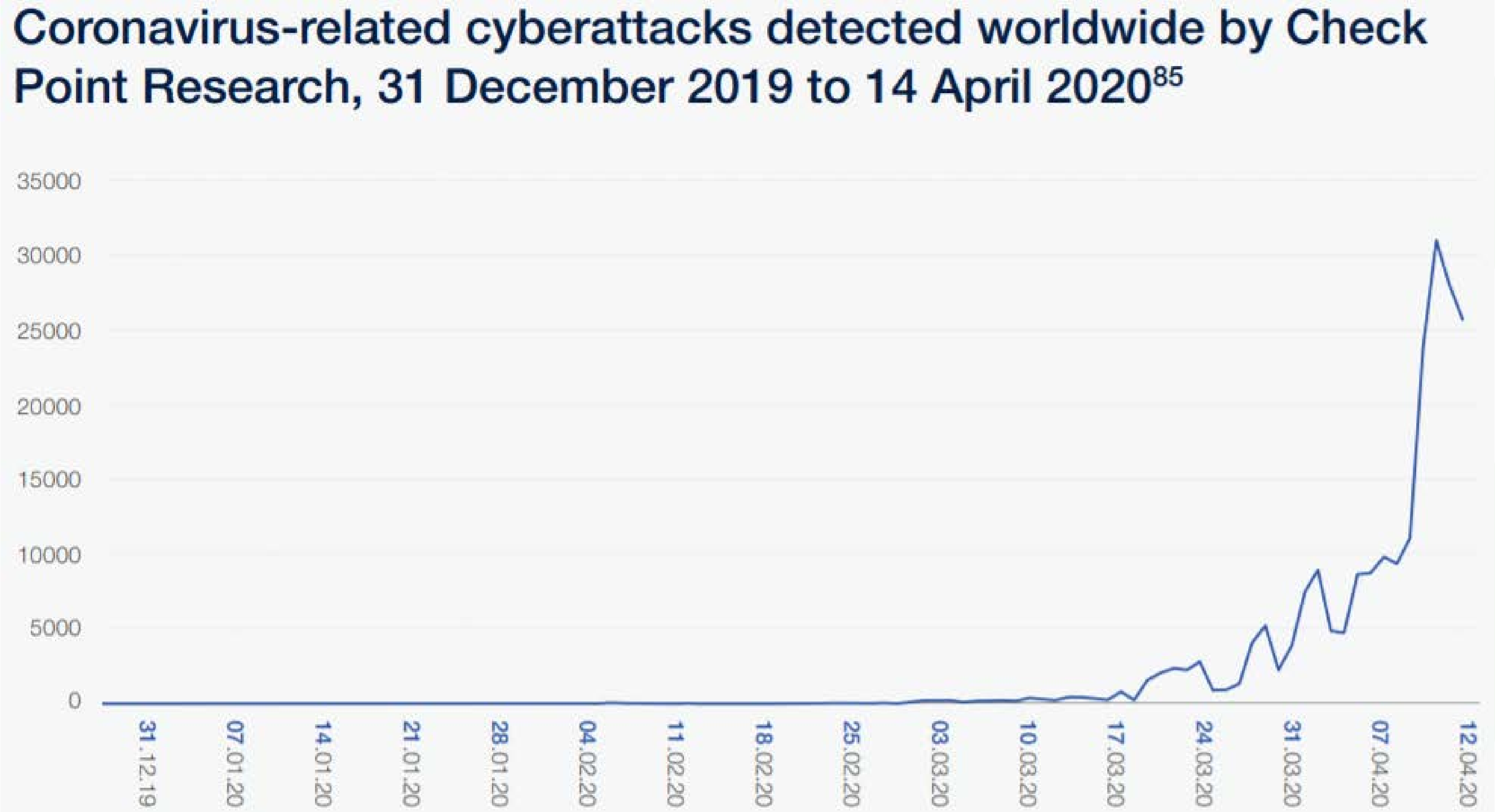
cybersecurity deals with precautions taken to guard against crime, which includes monitoring for suspicious network access attempts and steps taken to handle such attempts

Cybersecurity is a subgroup within the information security domain

Most worrisome risks for your company



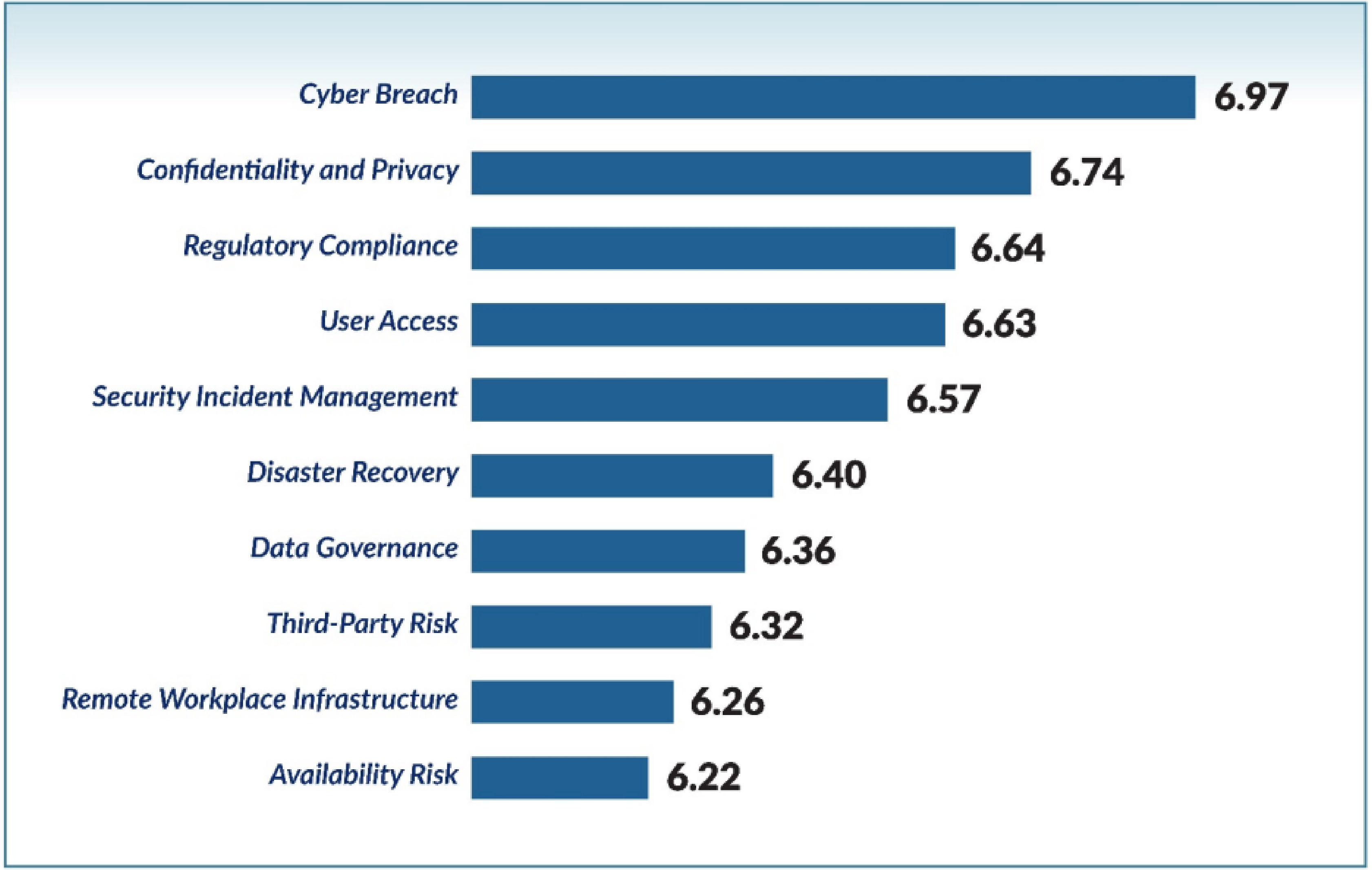
Cyberattacks detected



Coronavirus-related cyberattacks detected worldwide by Check Point Research, 31 December 2019 to 14 April 2020[85]

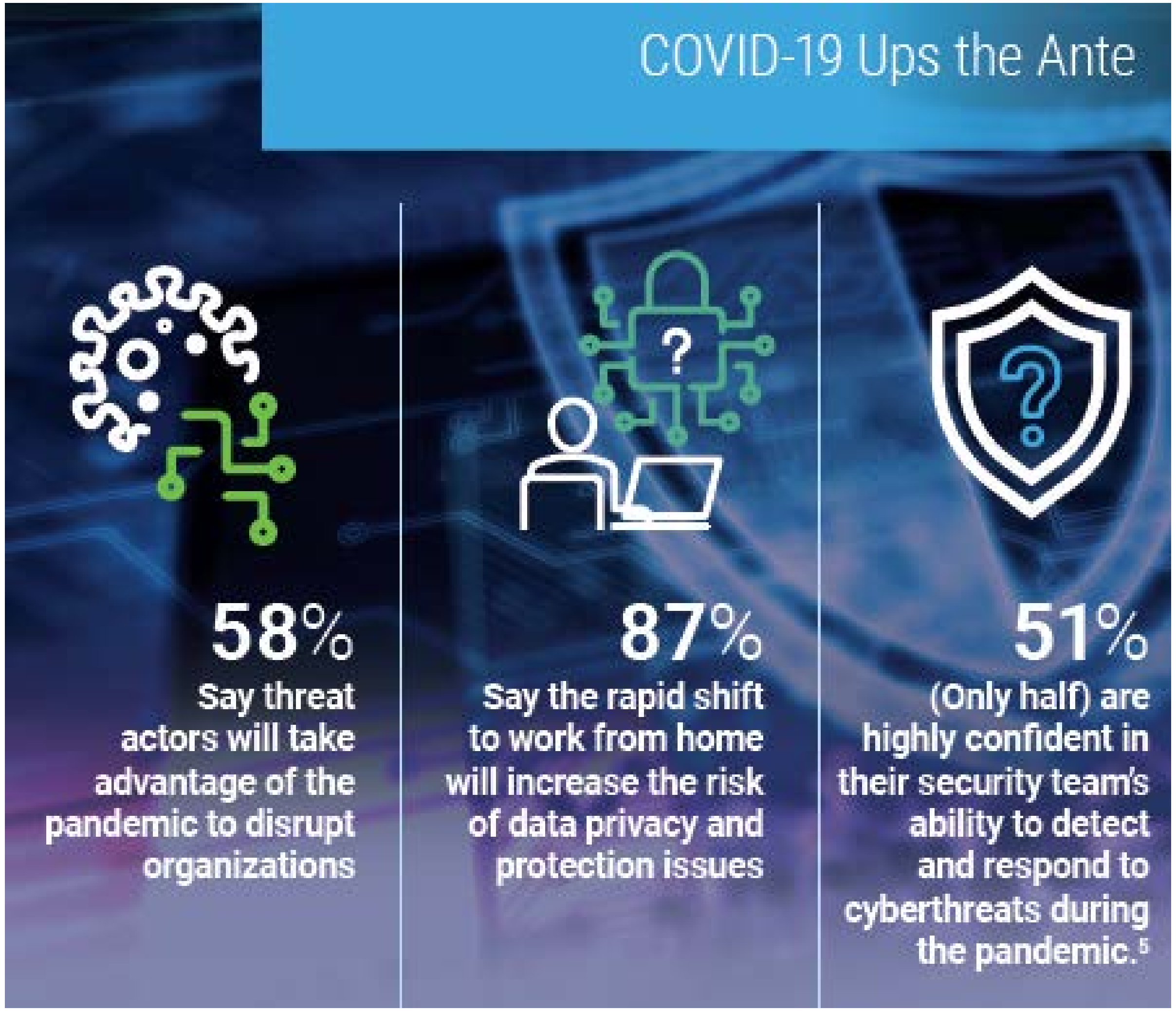
Importance of Cyber Resilience

Global Top 10 Technology Risks for 2021*



* *About our top technology risks scale*: Respondents were asked to rate the significance of 39 technology risk issues on a scale of 1 to 10, based on their organization's technology risk assessment, with "1" representing low impact to the organization and "10" representing extensive impact to the organization. Data points represent the mean score.

IT Audit's Perspectives on the Top Technology Risks for 2021

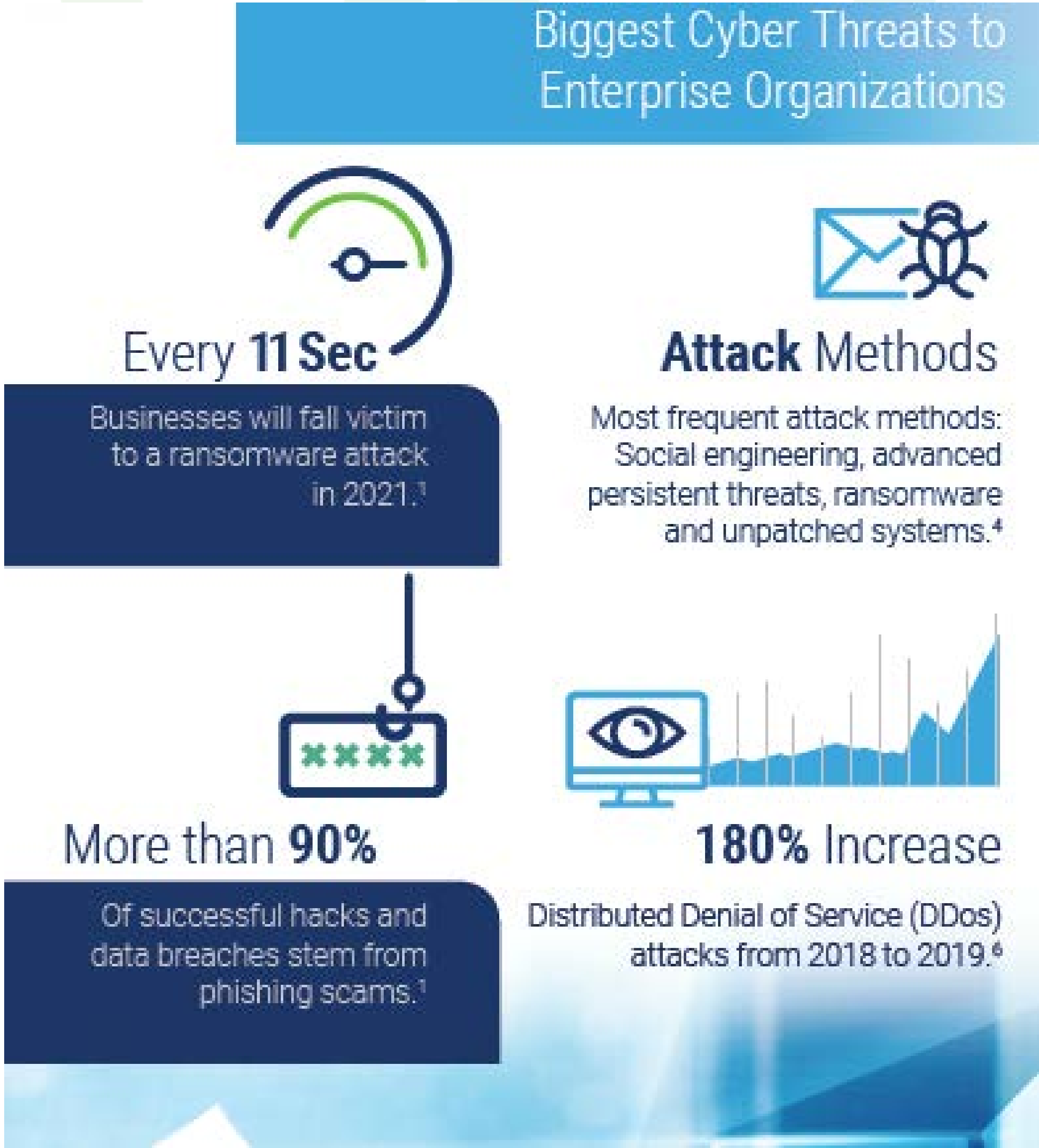


COVID-19 Ups the Ante

58% Say threat actors will take advantage of the pandemic to disrupt organizations

87% Say the rapid shift to work from home will increase the risk of data privacy and protection issues

51% (Only half) are highly confident in their security team's ability to detect and respond to cyberthreats during the pandemic.[5]



Biggest Cyber Threats to Enterprise Organizations

Every 11 Sec

Businesses will fall victim to a ransomware attack in 2021.[1]

Attack Methods

Most frequent attack methods: Social engineering, advanced persistent threats, ransomware and unpatched systems.[4]

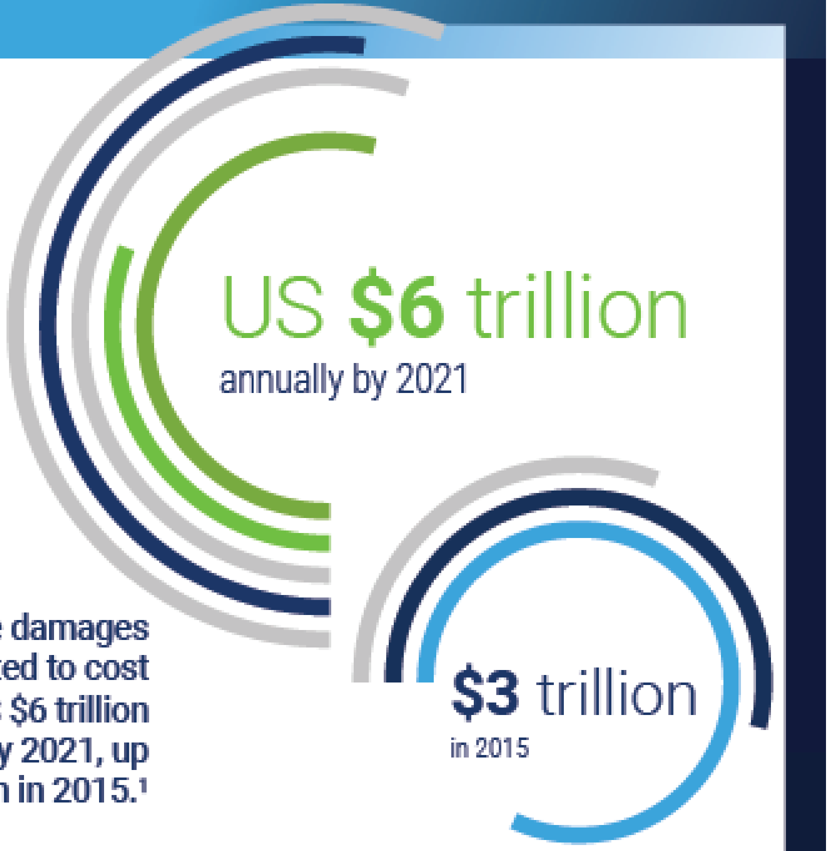
More than 90%

Of successful hacks and data breaches stem from phishing scams.[1]

180% Increase

Distributed Denial of Service (DDos) attacks from 2018 to 2019.[6]

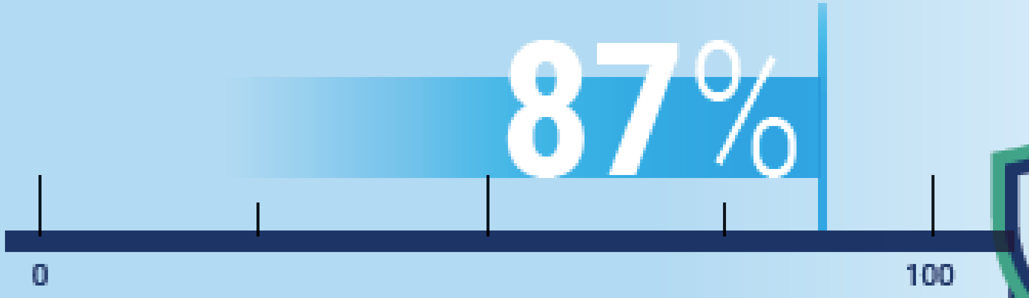
Much is at Stake ...



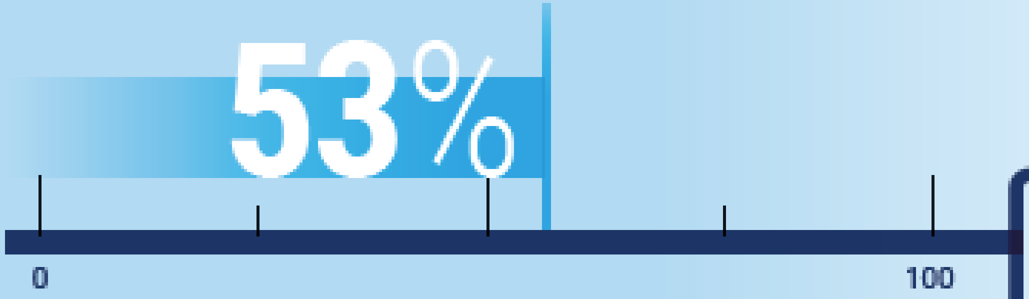
Cybercrime damages are projected to cost the world US $6 trillion annually by 2021, up from $3 trillion in 2015.[1]

60% OF SMALL COMPANIES THAT SUFFER A CYBERATTACK ARE OUT OF BUSINESS WITHIN 6 MONTHS.[2]

... But Confidence Is in Short Supply

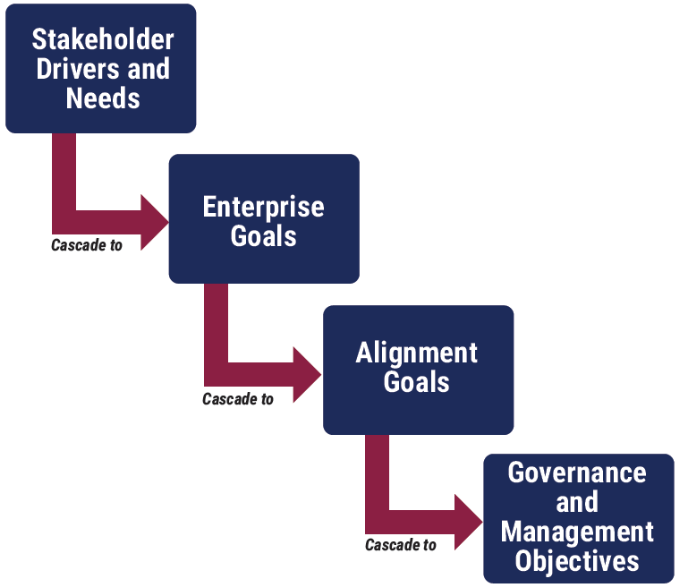


of C-Suite professionals and board members lack confidence in their company's cybersecurity capabilities.[3]



of security professionals believe it is likely their enterprise will experience a cyberattack in the next 12 months.[4]

I&T Governance: setting the tone at the top



Stakeholder Drivers and Needs

Cascade to

Enterprise Goals

Cascade to

Alignment Goals

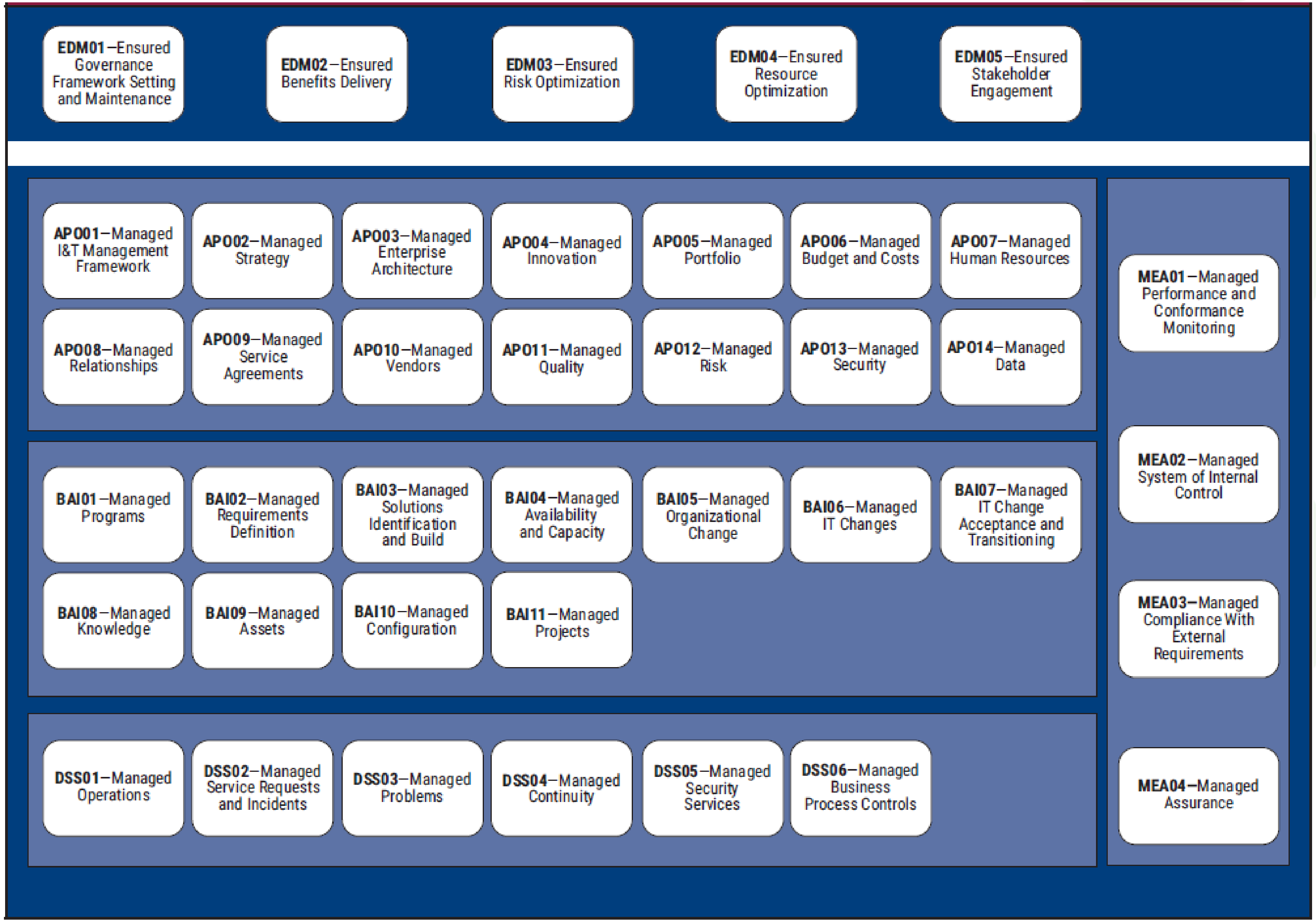
Cascade to

Governance and Management Objectives

Security Governance Frameworks from: ISACA, ISO, NIST, ISF, PCI SSC

ISACA®
Moscow Chapter

COBIT 2019 - I&T Governance Framework



EDM01–Ensured Governance Framework Setting and Maintenance

EDM02–Ensured Benefits Delivery

EDM03–Ensured Risk Optimization

EDM04–Ensured Resource Optimization

EDM05–Ensured Stakeholder Engagement

APO01–Managed I&T Management Framework

APO02–Managed Strategy

APO03–Managed Enterprise Architecture

APO04–Managed Innovation

APO05–Managed Portfolio

APO06–Managed Budget and Costs

APO07–Managed Human Resources

APO08–Managed Relationships

APO09–Managed Service Agreements

APO10–Managed Vendors

APO11–Managed Quality

APO12–Managed Risk

APO13–Managed Security

APO14–Managed Data

BAI01–Managed Programs

BAI02–Managed Requirements Definition

BAI03–Managed Solutions Identification and Build

BAI04–Managed Availability and Capacity

BAI05–Managed Organizational Change

BAI06–Managed IT Changes

BAI07–Managed IT Change Acceptance and Transitioning

BAI08–Managed Knowledge

BAI09–Managed Assets

BAI10–Managed Configuration

BAI11–Managed Projects

DSS01–Managed Operations

DSS02–Managed Service Requests and Incidents

DSS03–Managed Problems

DSS04–Managed Continuity

DSS05–Managed Security Services

DSS06–Managed Business Process Controls

MEA01–Managed Performance and Conformance Monitoring

MEA02–Managed System of Internal Control

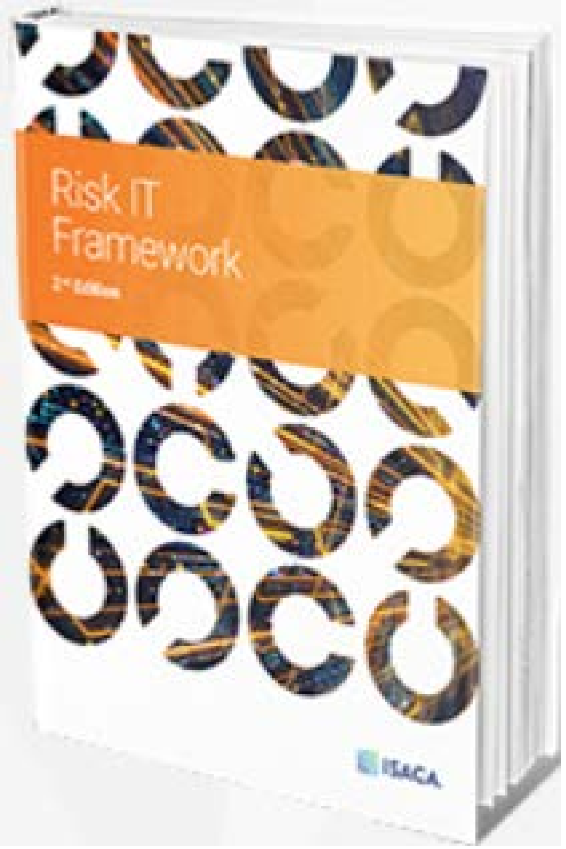
MEA03–Managed Compliance With External Requirements

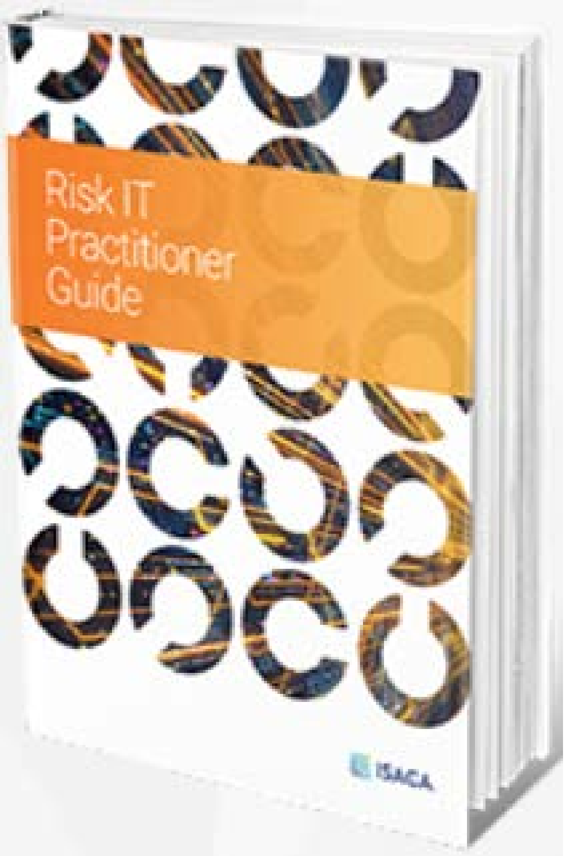
MEA04–Managed Assurance

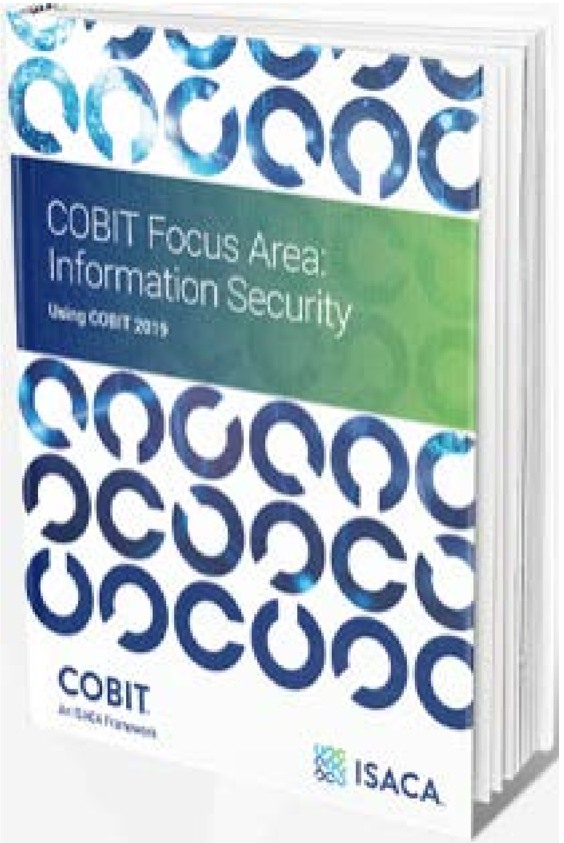
COBIT 2019
Introduction and Methodology
ISACA
COBIT 2019
Governance and Management Objectives
ISACA
COBIT 2019
Designing an Information and Technology Governance Solution
ISACA
COBIT 2019
Implementing and Optimizing an Information and Technology Governance Solution
ISACA

ISACA®
Moscow Chapter

Security Governance: New Publications





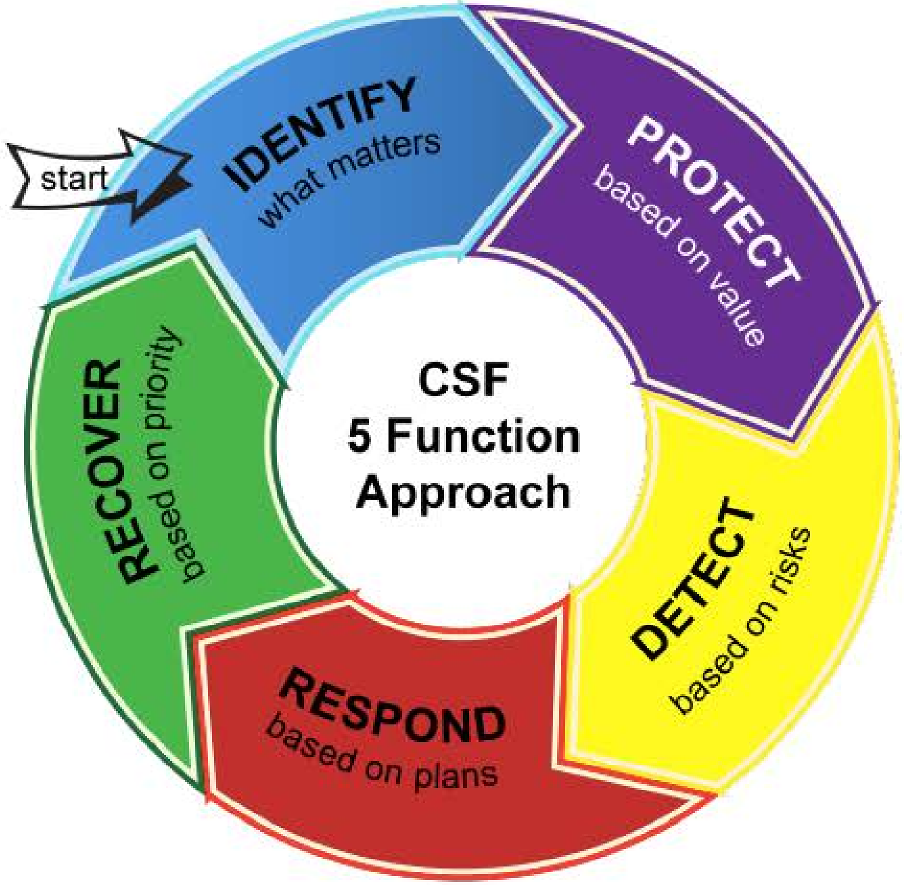


COBIT 2019
Implementing the NIST Cybersecurity Framework Using COBIT 2019
ISACA

ISACA
Moscow Chapter

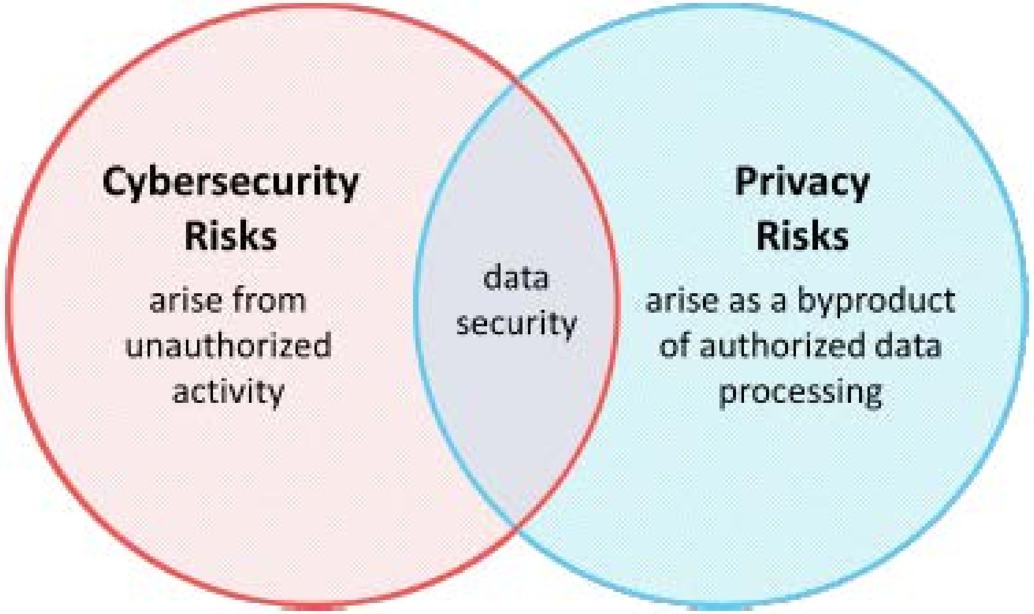
Framework for Improving Critical Infrastructure Cybersecurity (aka the Cybersecurity Framework)

- Released in 2014 with an update in 2017
- Provides a high-level model for discussing and coordinating cybersecurity activities
- Built around 5 straightforward functions, 23 categories, and 108 subcategories
- Goals are documented, current status is determined, and in light of risks, target activities & action plan are developed

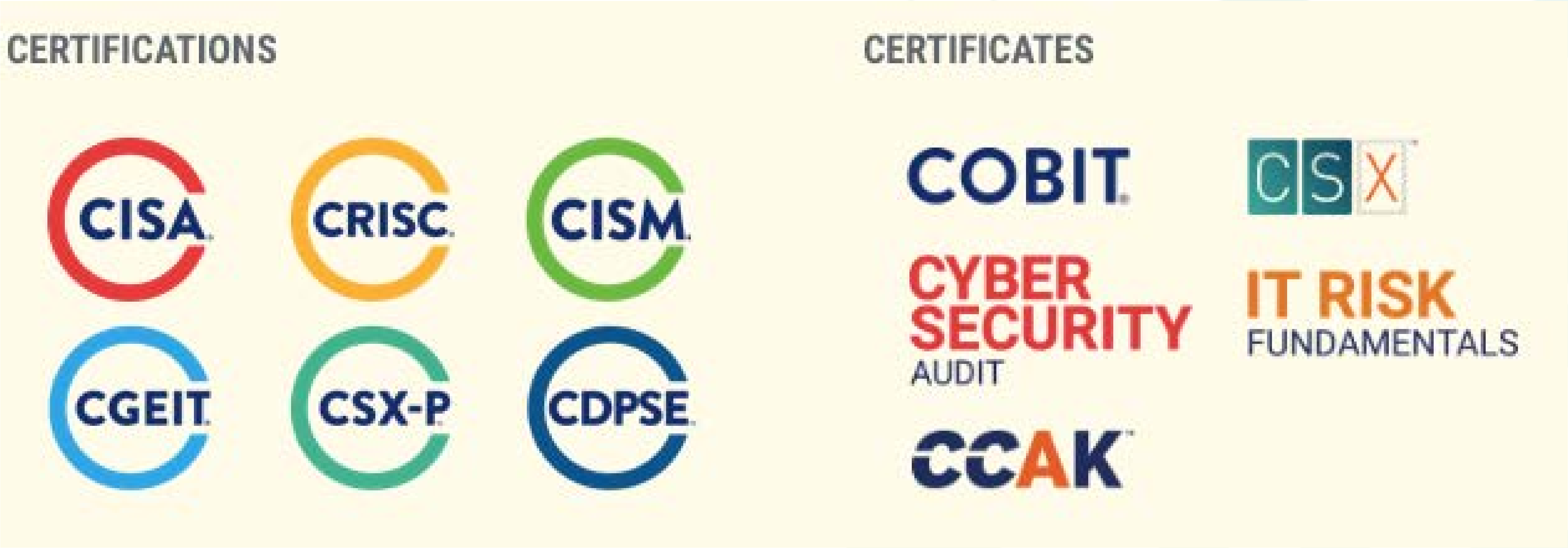


NIST Privacy Framework

- Similar model for organizing and communicating about relationship between Cybersecurity & Privacy Risk
- Recognition that data security has an important role in privacy protection
- Individual privacy cannot be achieved solely by securing data
- Authorized processing: system operations that handle data (collection – disposal) to enable the system to achieve mission/business objectives


Cybersecurity Risks
arise from unauthorized activity
data security
Privacy Risks
arise as a byproduct of authorized data processing

I&T Governance: Credentialing



CERTIFICATIONS

CISA

CRISC

CISM

CGEIT

CSX-P

CDPSE

CERTIFICATES

COBIT

CSX

CYBER SECURITY AUDIT

IT RISK FUNDAMENTALS

CCAK

ISACA
Moscow Chapter

ISACA®

Moscow Chapter