Ransomware Preparedness

Presented By:

DINDO GERON,

(CPHIMS, CISA, CISM, CRISC, NIA, CC, ITIL, COBIT)

JANUARY 27, 2024

DOHA - QATAR

Table of Contents

Topics we will cover (30 Mins)

1. Backup Is King for Cyber Recovery

ESG, a technology research firm conducted a survey study in 2022:

620

IT & Cybersecurity Professional

Mid-Market and Enterprise Org

North America Western Europe

Planned method(s) of recovery from successful ransomware attack for impacted applications and data.

41%

Restore from our standard data protection/ backup solution

39%

Restore from public cloud services

37%

Restore from air-gapped/ isolated protection storage

36%

Restore from disaster recovery service provider

35%

Restore from an immutable backup/gold copy

54%

Restore from both on-premises and public cloud resources

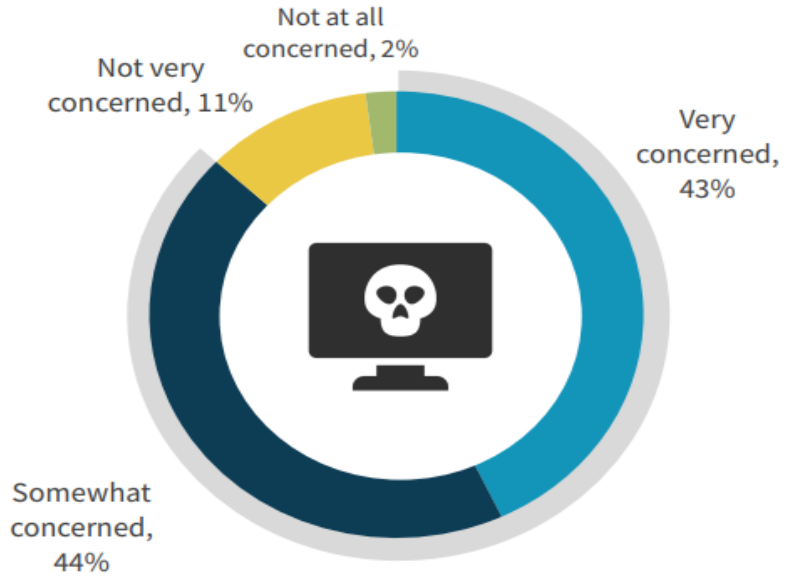
47%

Restore from both on-premises and public cloud resources

55%

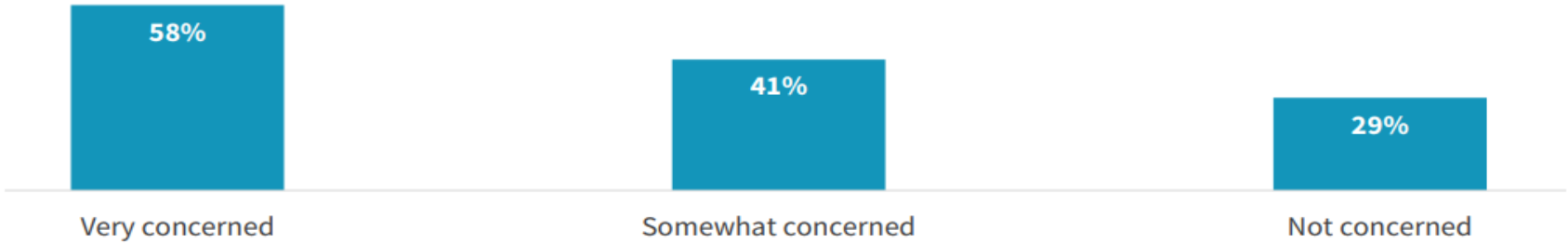
Restore from both on-premises and public cloud resources

Level of concern that data protection copies could also become corrupted by ransomware attacks.

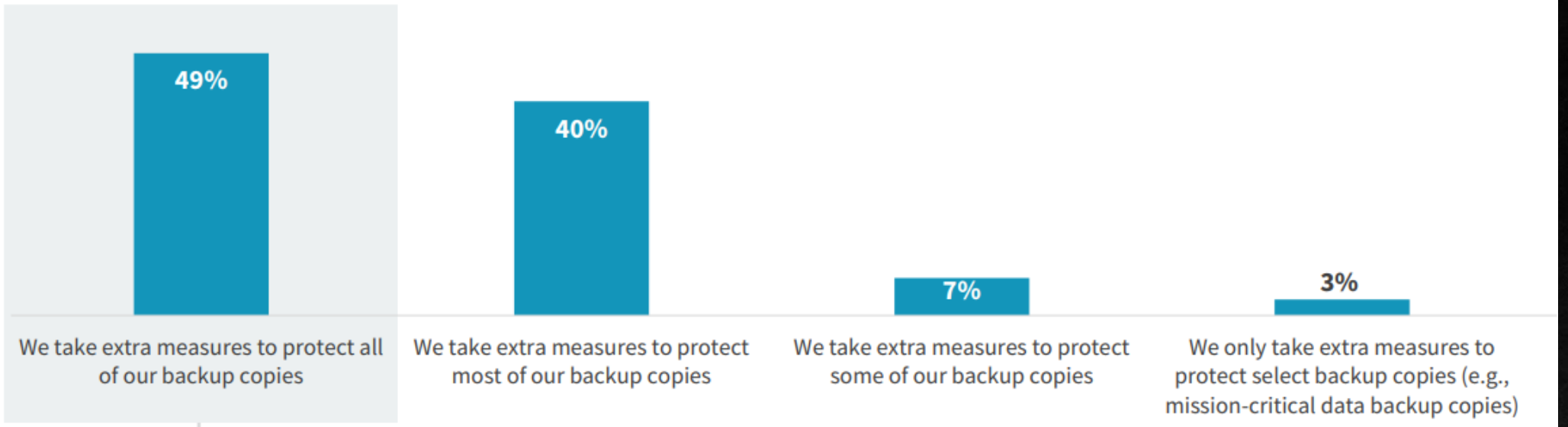


47% leverage a third-party tool to automate data backup restoration, configuration, and validation.

Percentage of organizations that leverage a third-party backup validation tool based on level of concern that data protection copies could become infected.



Extent to which backup copies of data are protected against ransomware attacks.



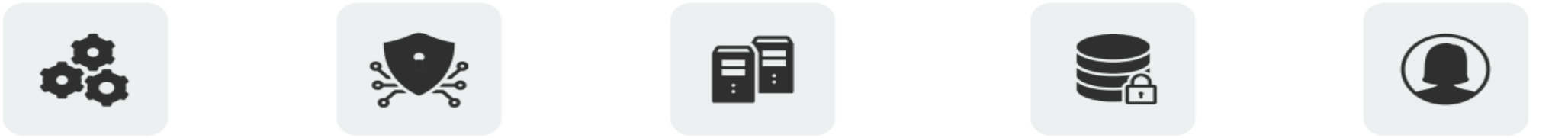
“There is still significant room to grow overall with only 49% reporting that they take extra measures for all their backup copies.”

Back it UP!
Repeat that several times and Protecting Backup Copies Is a Key Prevention Tactic

- Take regular **OFFLINE backups**
- Use **HYBRID Recovery Methodologies**
- Apply **AIR-GAPPING** for your backup
- Invest in **IMMUTABLE backup technology**

2. Ransomware Readiness Is a Team Sport

Groups that contribute funding to technologies for ransomware readiness.



60% IT operations budget

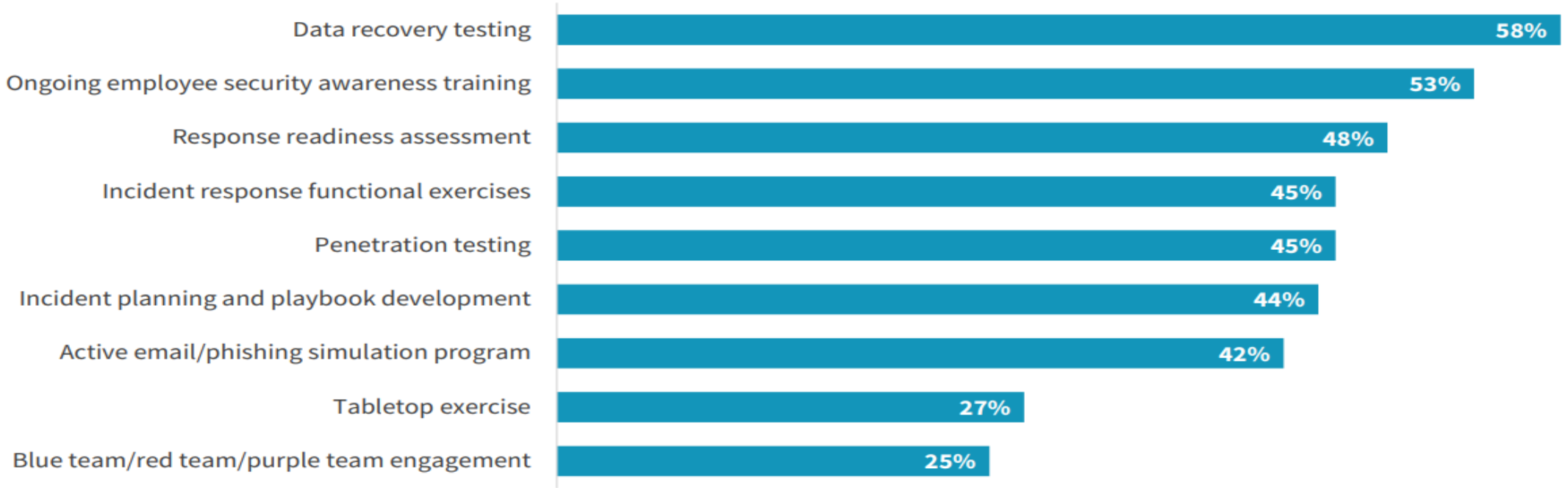
56% Cybersecurity/ information security team budget

52% General IT budget

39% Data protection budget

32% Executive-level budget

Ongoing ransomware preparedness activities and processes.



Preparedness to mitigate the impact of ransomware.

52%

Our preparedness position for ransomware is much stronger today than it was two years ago

47%

Our preparedness position for ransomware is somewhat stronger today than it was two years ago

Importance of ransomware preparedness for executive team and/or board of directors.

26%

The most important business priority

53%

One of the top 5 business priorities

Expected spending on ransomware preparedness over the next 12-18 months.

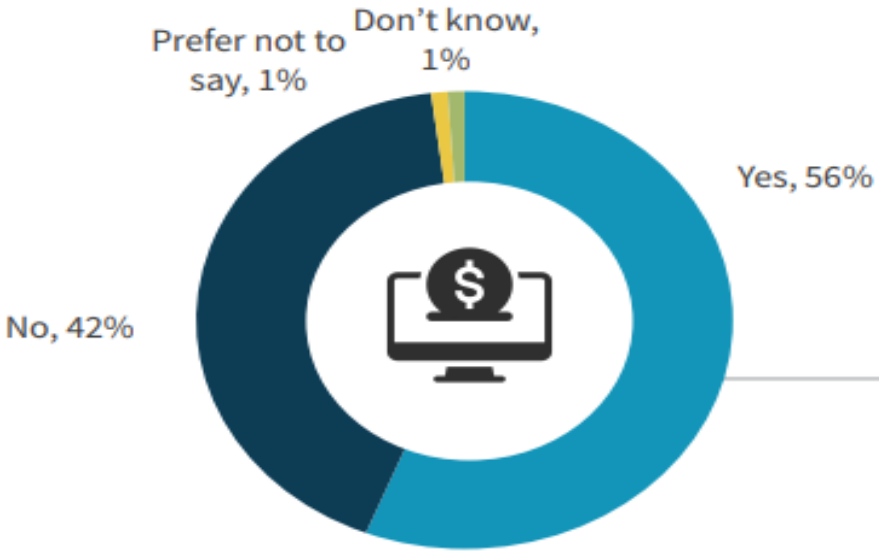
35%

Increase significantly

47%

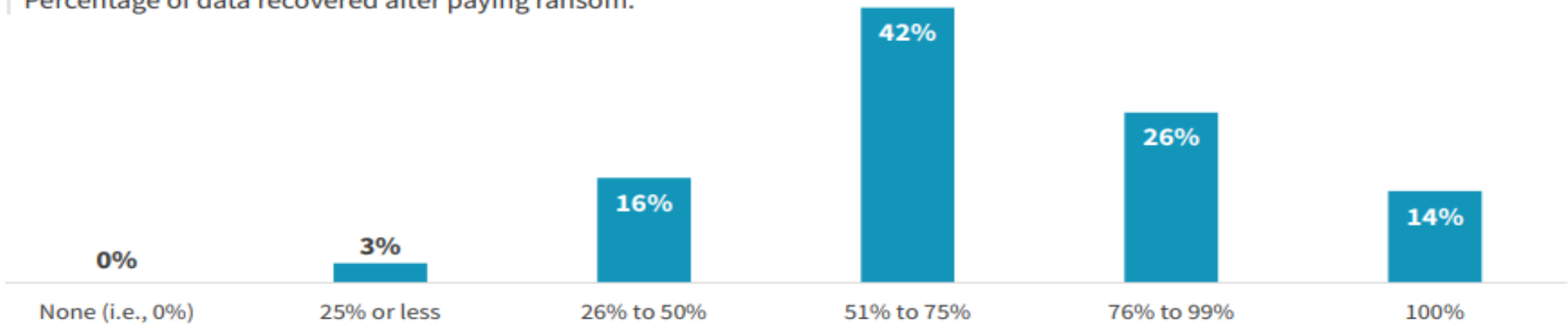
Increase slightly

Have organizations paid ransoms resulting from successful attacks?

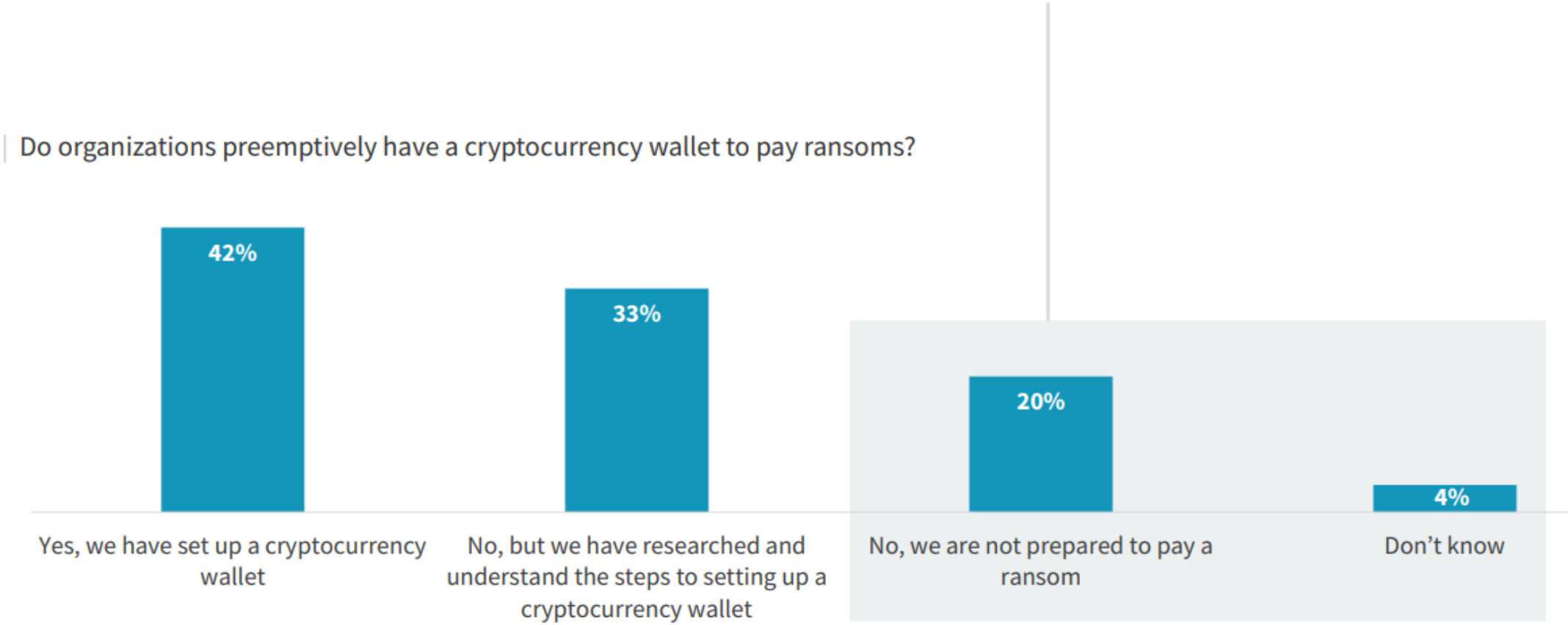


More than half of organizations that have been victimized by a successful ransomware attack at some point admit to having paid a ransom to regain access to data, applications, or systems."

Percentage of data recovered after paying ransom.



“Nearly a quarter seem to be **unprepared to pay a ransom.**”



Be Prepared!
Optimize your response activities
Repeat that several times, practice makes perfect as they say

- **Validate your Backup**, test FULL recovery on a regular basis
- Run Ransomware **Tabletop Exercises** regularly with management and technical teams
- Conduct **Cyber Incident Planning & Response training** and workshops for your technical and management teams.
- Run **Cyber Crisis Awareness Exercises** for your senior leadership and board members

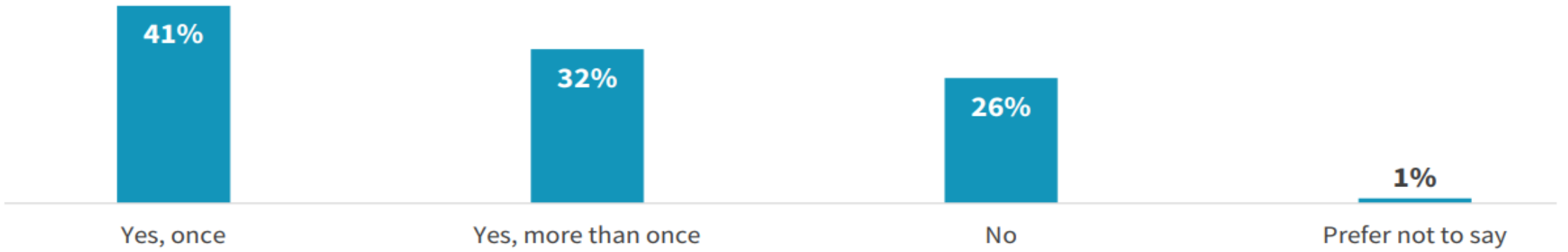
Comply with the regulations imposed by the Government of Qatar

- **National Cybersecurity Strategy 2023-2028**, which aims to protect Qatar's cyberspace from threats and risks,
- **Personal Data Privacy Law 2016**, which regulates the collection, processing and transfer of personal data,
- **Electronic Commerce Law 2010**, which governs online transactions and contracts,
- **Cybercrime Prevention Law 2014**, which criminalizes various acts of cybercrime such as hacking, fraud and identity theft.

3. Preventative & Detective Security Controls are Critical to Ransomware Preventions, Yet Significant Gaps Exist for Most

Attempted ransomware attack frequency over the past 12 months.

Successful ransomware attacks over the past 12 months.



Areas of IT environment impacted by successful ransomware attack(s).

40% Storage systems

39% Cloud-based data

37% Networks or connectivity

36% Key IT infrastructure

36% Data protection infrastructure

53%
of victims of successful ransomware attacks report that this **included sensitive infrastructure configuration data.**

Initial point of compromise for successful ransomware attack(s).

36% Application software vulnerability

33% Systems software vulnerability

31% Application user permissions and misconfigurations

31% Misconfiguration of externally exposed device

27% Email

Most critical preventative security controls for protecting against ransomware.

43%
Network security

40%
Backup infrastructure security

39%
Endpoint security

36%
Email security

36%
Data encryption

33%
Identity and access controls such as multi-factor authentication, privileged access management, etc.

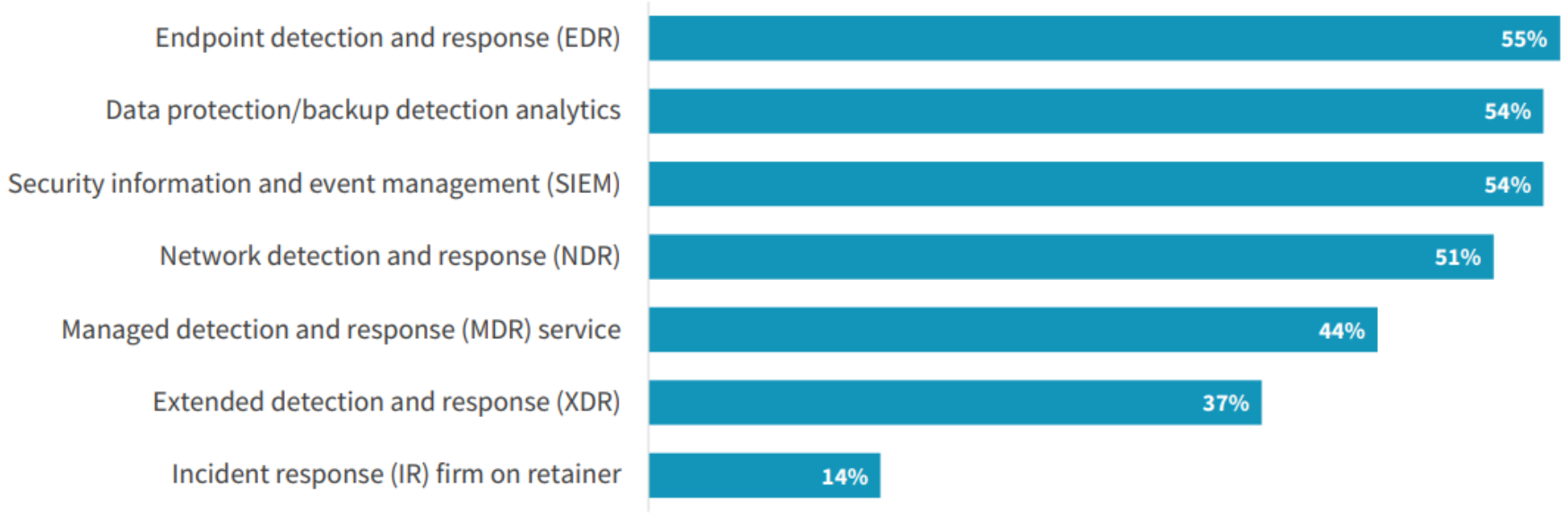
28%
Internet-of-things security

27%
Identity prevention systems/ identity detection systems

27%
Vulnerability management

23%
Automated data security audits and progress reports

Mechanisms in place to help detect and respond to an active ransomware attack.



Who handles incident response in the event of a ransomware attack?

63%

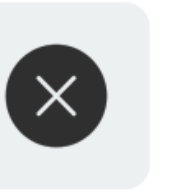
Our own internal IR resources

53%

We use our MDR provider for IR

13%

IR firm we have on retainer



2%

We have no IR capabilities in place

Paying ransom doesn't guarantee Data Recovery So backup is critical in business resumption, + Strong Vulnerability Management programs

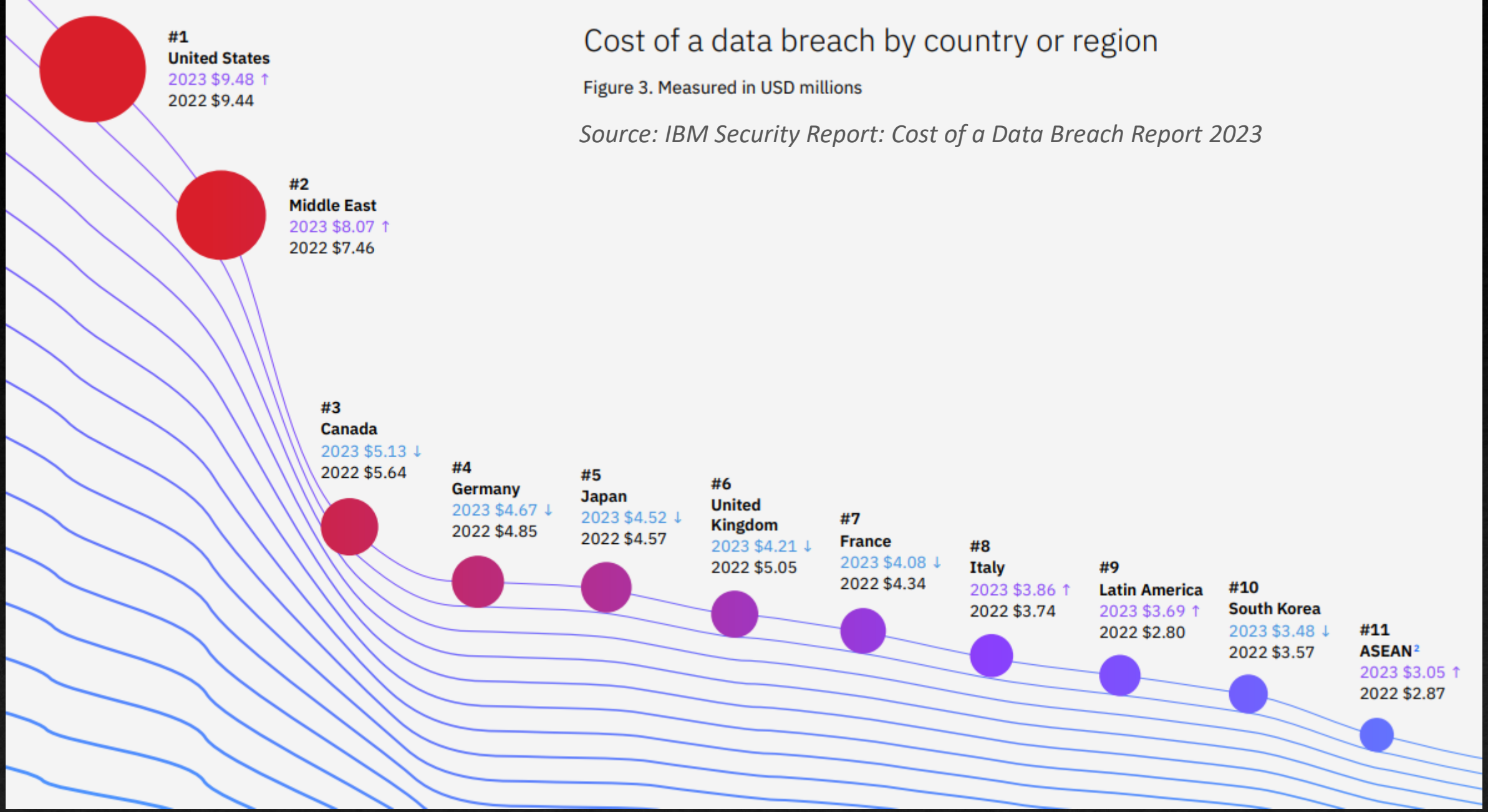
- **Protect the Master Keys,** manage and monitor all **Privileged Credentials** and the users who have access to them. No excuses!
- **Be Normal, Login Normal**. For their day-to-day tasks (email, browsing etc) mandate that privileged users. DO NOT login with their privileged credentials. Again, no excuses.
- **Authenticate with Multi Factors**. As a minimum FORCE, all technical and business privileged users must use MFA or multi-factor authentication. Avoid SMS as a password delivery medium for the 2FA.
- **Updates**. Without exception, ALL operating systems must have critical severity and security patches applied within 14 days or less after they are made available.

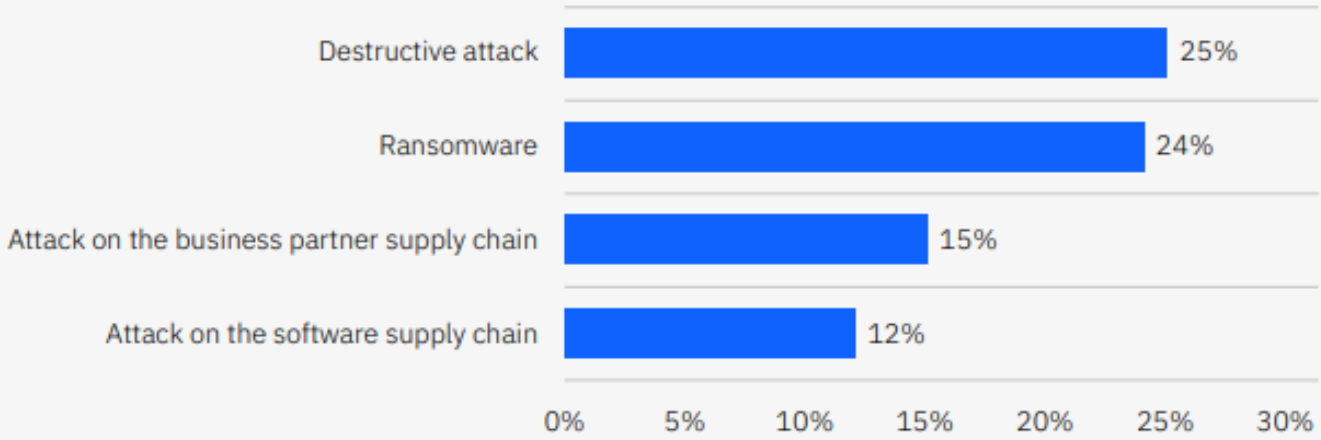
4. Intro to Cyber Insurance as a Preemptive Ransomware Measure

Cost of a data breach by country or region

Figure 3. Measured in USD millions

Source: IBM Security Report: Cost of a Data Breach Report 2023





Source: IBM Security Report:
Cost of a Data Breach Report 2023

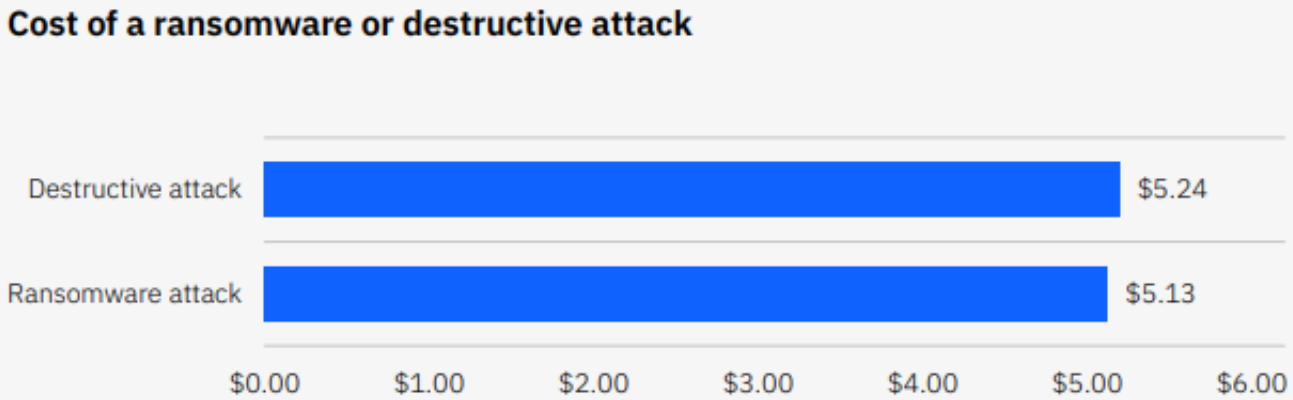
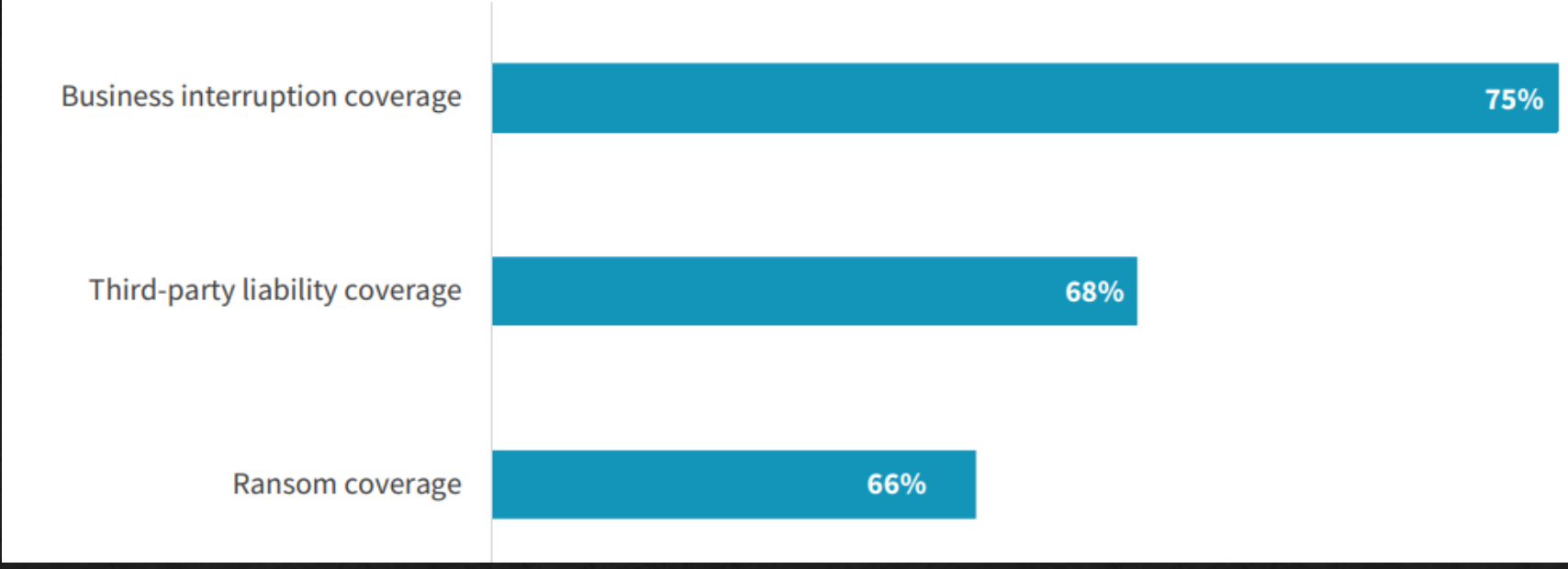


Figure 20. Measured in USD millions

More than one-third (35%) of organizations report they currently purchase cyber insurance as a ransomware mitigation tactic."

Type(s) of cyber insurance to which organizations currently subscribe.



WHAT SHOULD YOUR CYBER INSURANCE POLICY COVER?

Make sure your policy includes coverage for:

- ☐ Data breaches (like incidents involving theft of personal information)
- ☐ Cyber attacks on your data held by vendors and other third parties
- ☐ Terrorist acts
- ☐ Cyber attacks (like breaches of your network)
- ☐ Cyber attacks that occur anywhere in the world

Also, consider whether your cyber insurance provider will:

- ☐ Defend you in a lawsuit or regulatory investigation (look for "duty to defend" wording)
- ☐ Provide coverage in excess of any other applicable insurance you have
- ☐ Offer a breach hotline that's available every day of the year at all times

WHAT IS

FIRST-PARTY COVERAGE

AND WHAT SHOULD YOU LOOK FOR?

First-party cyber coverage protects your data, including employee and customer information. This coverage typically includes your business's costs related to:

- ☐ Legal counsel to determine your notification and regulatory obligations
- ☐ Customer notification and call center services
- ☐ Crisis management and public relations
- ☐ Forensic services to investigate the breach
- ☐ Recovery and replacement of lost or stolen data
- ☐ Lost income due to business interruption
- ☐ Cyber extortion and fraud
- ☐ Fees, fines, and penalties related to the cyber incident

WHAT IS THIRD-PARTY COVERAGE AND WHAT SHOULD YOU LOOK FOR?

Third-party cyber coverage generally protects you from liability if a third party brings claims against you. This coverage typically includes:

- ☐ Payments to consumers affected by the breach
- ☐ Claims and settlement expenses relating to disputes or lawsuits
- ☐ Losses related to defamation and copyright or trademark infringement
- ☐ Costs for litigation and responding to regulatory inquiries
- ☐ Other settlements, damages, and judgments
- ☐ Accounting costs

Collaborate with your Insurance Broker and Cybersecurity Vendor
Layer your Security Controls to meet your cyber insurance requirements

- **Collaborate with your broker,** to determine your coverage eligibility, what is covered, excluded, or endorsement requirements, cost of your premiums, and renewal eligibility
- **Identify your RISKS**. Which data or application requires protection. Deploy security measures and Pen-Test to estimate your net-risk.

Being prepared helps in achieving goals and in avoiding and mitigating negative outcomes.

- **What will the future of ransomware bring?**
- **Has it reached its tipping point?**
- **What will the next big attack vector be?**
- **Who will the next victim be?**

THANK YOU

References:

1. *ESG Research Firm Survey : The Long Road Ahead to Ransomware Preparedness (theregister.com)*
2. *IBM Security Study: Cost of a data breach 2023 | IBM*
3. *NISCF_booklet_2020_EN.pdf (ncsa.gov.qa)*
4. *Law No.13 of 2016 (ncsa.gov.qa)*
5. *Qatar's e-Commerce Law | Ministry of Communications and Information Technology (mcit.gov.qa)*
6. *Cybercrime Prevention Law No 14 of 2014 (cra.gov.qa)*