bluelock®

# State of IT Security, 2017

## Prevention & Recovery Practices

# Table of Contents



"Cybercriminals are making a living off targeting industries which are reliant upon information that needs to be readily available and strictly confidential. Preventative measures are key to securing your organization's IT systems, but not the whole picture as they cannot be foolproof to all threats at all times. Organizations must address restorative and results-oriented security solutions as well."

*– Derek Brost, Director of Engineering at Bluelock*

Based on IDG Research survey results commissioned by Bluelock
May 2017 survey titled "Quick Poll Research: *Disaster Recovery - An essential component of data protection*

# Survey Overview

Security incidents are a wide-spread issue, and companies are rightful to be wary of them. But what threats are organizations most concerned about, and what are they doing to mitigate these concerns?

Bluelock, a leading DRaaS provider protecting vast amounts of sensitive data, commissioned a survey from IDG Research (parent company of CIO Online, CSO Online, NetworkWorld, etc.) to assess the current state of IT security practices.

**Key Findings**

| Question | Result |
|---|---|
| Biggest concern resulting from a security breach | 64% of respondents cited "loss of customer confidence" |
| Top concern in a security incident | 44% of executive leadership claimed "inability to recover data and systems in less than a day" |
| Other major concerns in a security incident | 49% of respondents were concerned with "loss of sensitive data" during a security breach |
| Thoughts on IT disaster recovery | 64% of respondents believe that disaster recovery should be incorporated into an IT security strategy |

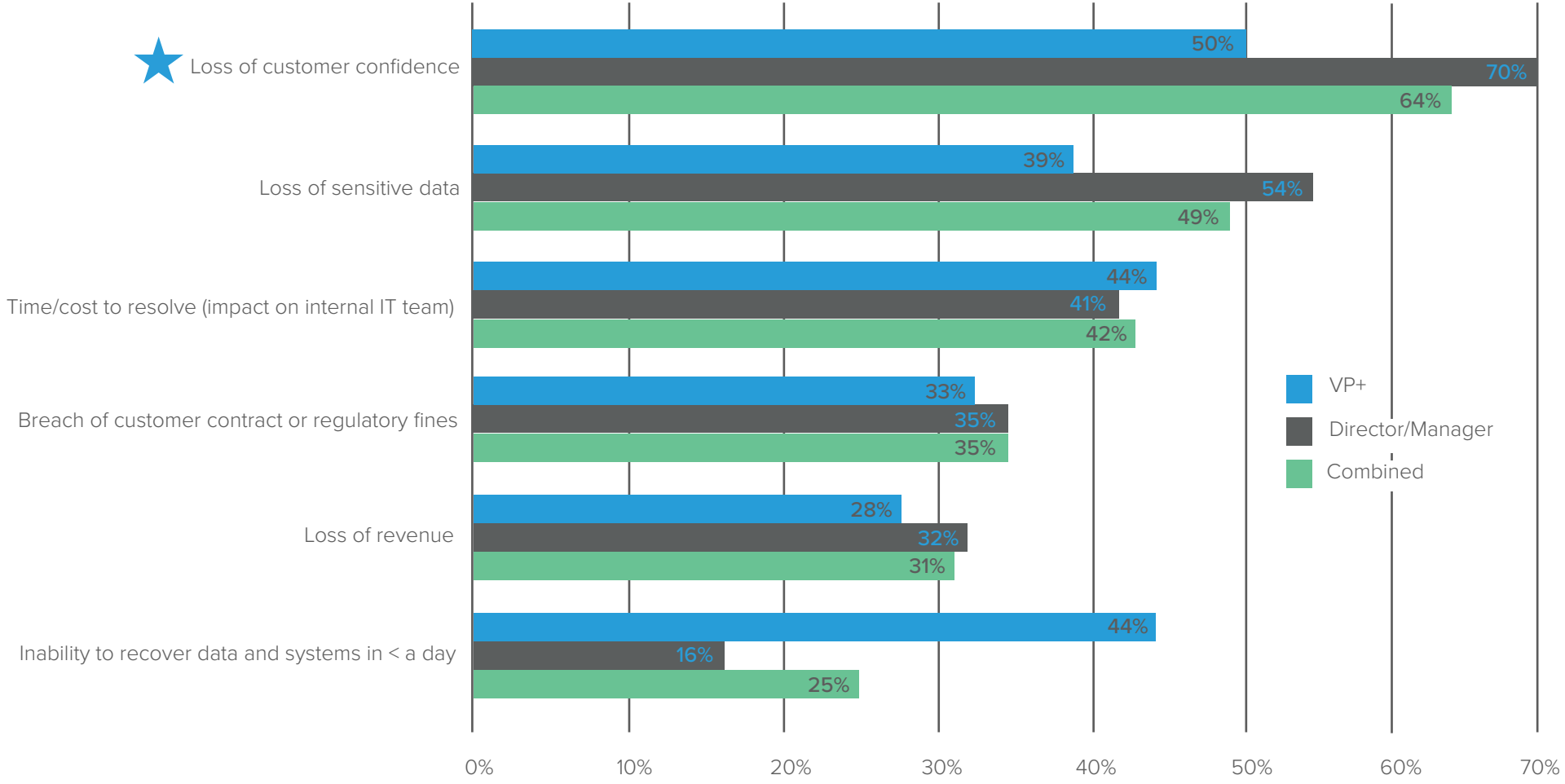
# Survey Results

## Top Threats and Risk Mitigation Priorities

bluelock®

# Top Concern: Loss of Customer Confidence

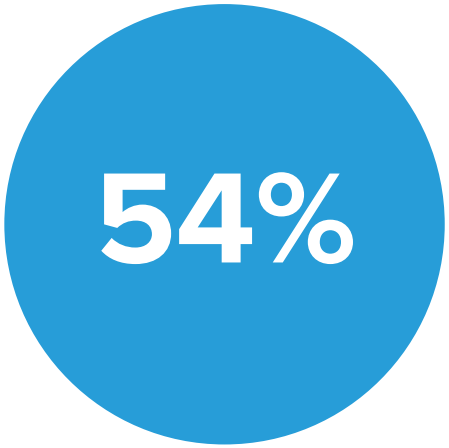
What are your organization's biggest concerns in the event of a security beach?




Both executive and IT manager respondents recognize the connection between "customer confidence" and organizational excellence. When customers or clients don't feel comfortable sharing their sensitive information with an organization, it has a rippling impact on business livelihood.

# Executives fear prolonged downtime - IT managers fear loss of sensitive data

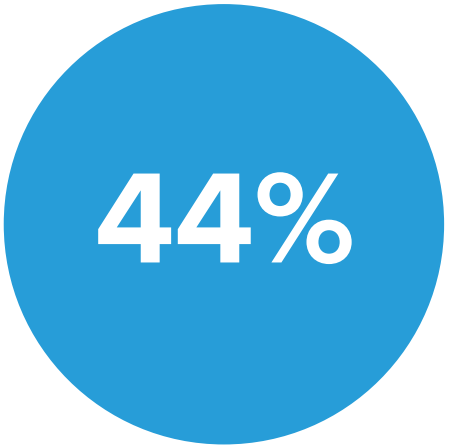
While all respondents agreed that loss of customer confidence is the most detrimental impact of a security breach, the secondary fear demonstrated a difference in priorities. Executives fear prolonged downtime, while IT managers fear loss of data. Both cause great pain to an organization, but they are also prevented by largely different IT investments.




Percentage of IT managers who care most about **loss of sensitive data**

*(their top concern after reputational impact)*

***Recommended IT Investment:*** IT disaster recovery for reactive/restorative measures




Percentage of executives who care most about **time-to-recovery** after a security incident

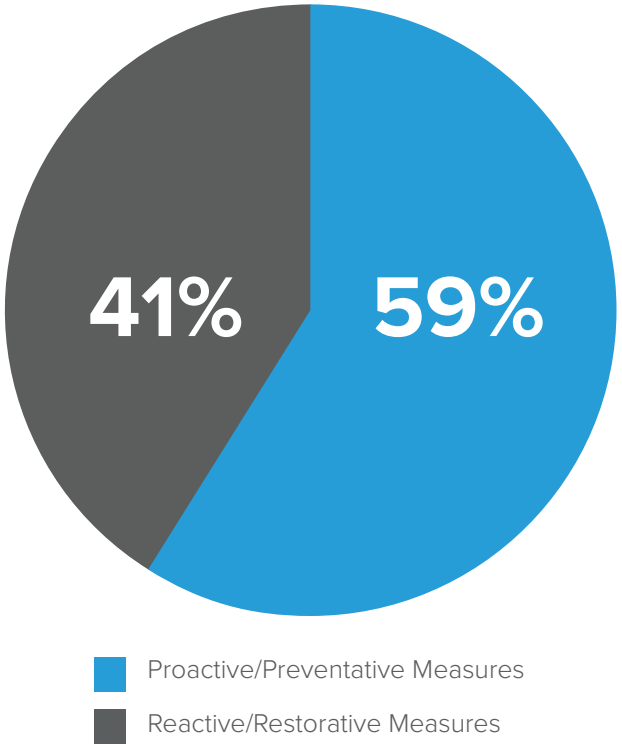
*(their top concern after reputational impact)*

***Recommended IT Investment:*** IT cybersecurity for proactive/preventative measures

What are your organization's biggest concerns in the event of a security breach?

# Preventative measures are currently prioritized over restorative measures

## Data Protection Approach



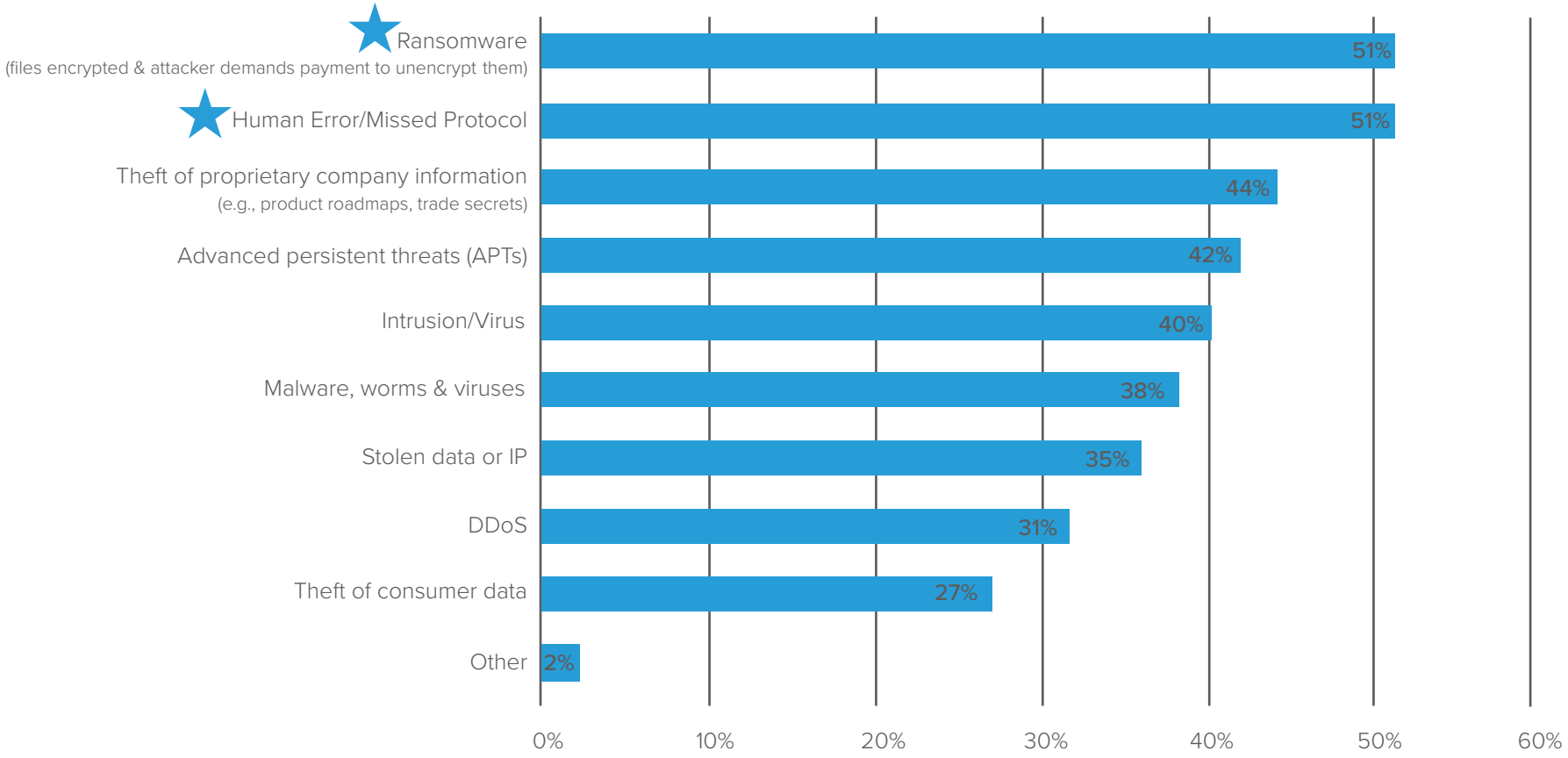

A holistic security strategy relies on organizations preventing security breaches and responding to them effectively. However, most IT teams are focused more on prevention. This creates risk because no organization can fully protect itself from all threats and ineffective IT-DR processes can result in prolonged downtime.

Thinking about your organization's approach to data protection and minimizing risk, to what extent is it focused on proactive/preventative measures versus reactive/restorative measures?

# Perceived threats demand restorative measures for risk mitigation

Ransomware, the biggest perceived security threat, is a prime example of a threat vector that can be alleviated with restorative measures in place. If the attacker encrypts production data, IT departments can avoid paying ransomware fines or losing data by accessing clean copies from their DR and backup site.

## What do you perceive to be your organization's biggest security threats today?



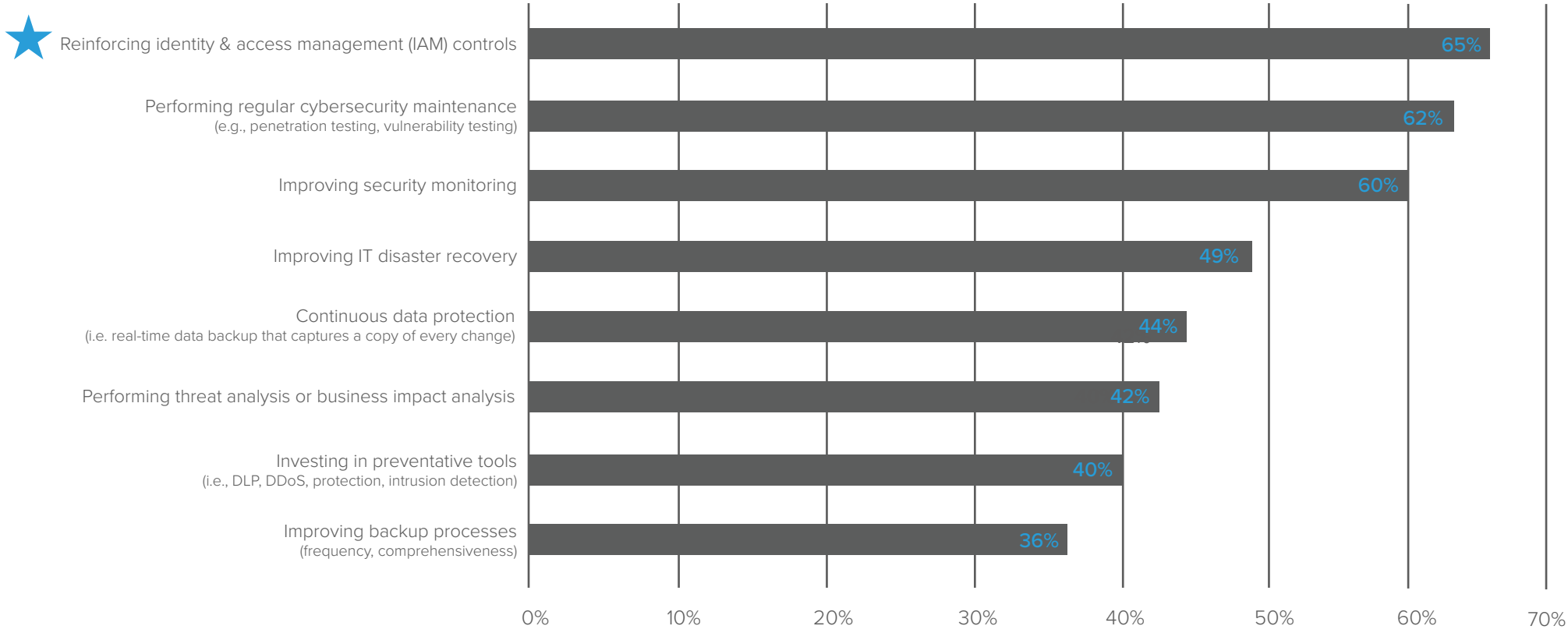



bluelock.

# Unfortunately, most companies are not prioritizing reactive measures

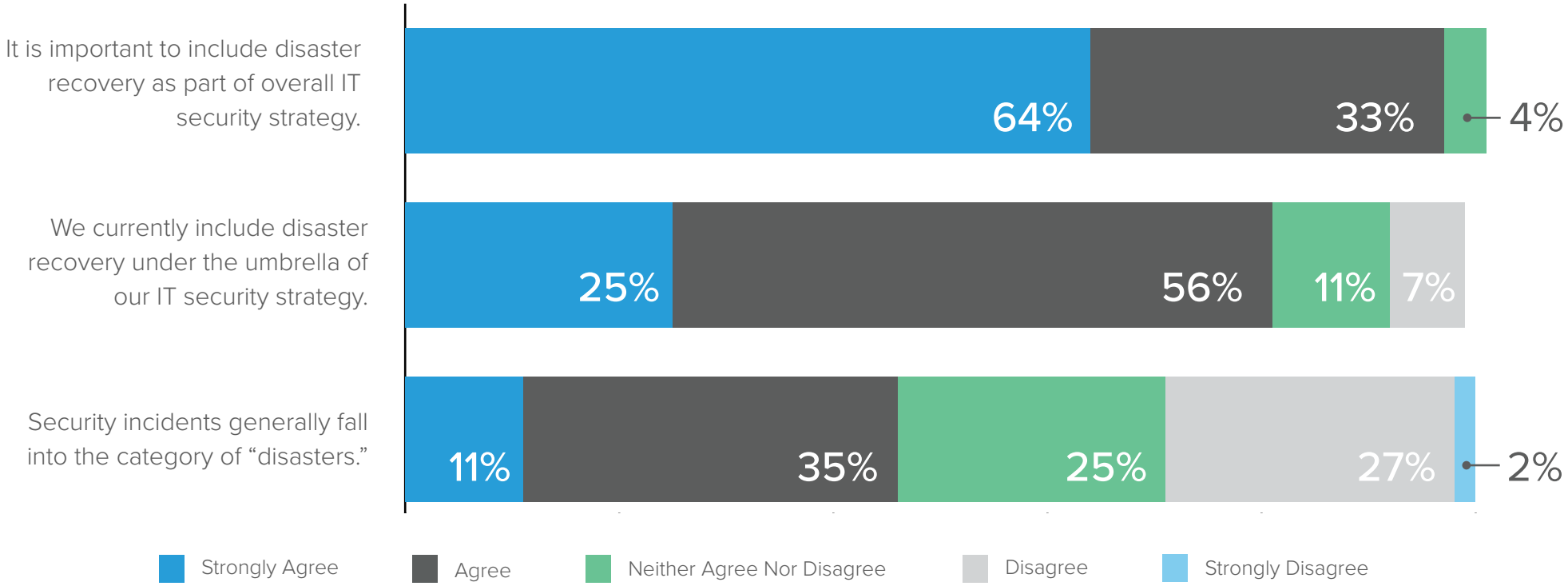
Proactive measures reigned as the top three priorities. IT disaster recovery, continuous data protection and backups were not named as a top-five priority by a majority of the respondents.

## What are your organization's top data protection priorities over the next 12 months?



# However, most believe IT-DR should be incorporated into an IT security strategy

Please rate your level of agreement with the following statements.




*"The reality is if your information system is taken down for whatever reason: a flood, malware, hack attack, etc., you still have a business continuity and disaster recovery issue on your hands."*

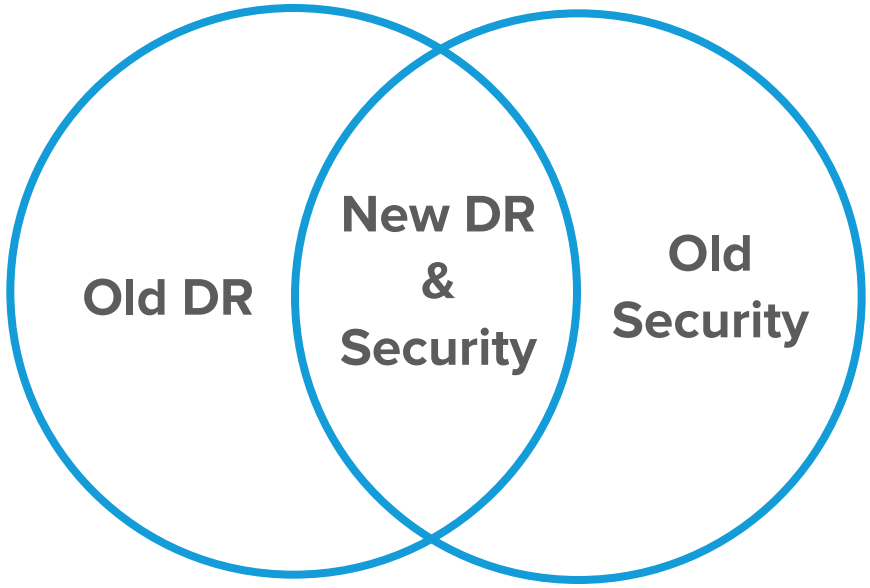
*- Ken Beaver, TechTarget*

# Conclusion

## How to leverage DRaaS for restorative efficacy

bluelock®

# DRaaS enables a holistic approach to security




Security professionals have historically viewed disaster recovery (DR) as an IT responsibility, but evolving circumstances in the security threat landscape are bringing DR and security plans closer and closer together. Now, companies need a collaborative approach and process for DR and security. This means that security specialists and IT personnel must co-own resiliency tasks to achieve full mitigation – something that both groups can facilitate with Disaster Recovery-as-a-Service (DRaaS).

## DRaaS is a solution for this convergence

- Data replication and backup to a secure off-site location
- Testing and documentation to make sure protection practices stay in sync
- Ongoing monitoring and encryption
- Team of experts for methodology, maintenance and recovery execution (ideal for overburdened IT teams)


Read our Practical Guide to Disaster Recovery-as-a-Service to learn more about how DRaaS can empower your security stance.