Is Your Organization Prepared for CYBER INCIDENTS?

Cyberattacks are **300 times** as likely to hit **Financial Institutions** than business from other industries

Source: Boston Consulting Group, 20 June 2019. For Wealth Managers, Off Year Sparks Opportunity to Reignite Growth
Overview: https://www.bcg.com/d/press/20june2019-global-wealth-report-222692

In the current trend, the growth of application and device capabilities to accommodate various online services leads to a higher risk of exposure to cyberattacks. Some common examples of online services include bank transfers, bill payments, online shopping, trip booking, and membership management.

Despite protective measures in place, there is no guarantee that an organization can be risk-free or immune to cyberattacks. These breaches come with a cost as recovering from a breach consumes time and money.

Current approaches for most organizations in incident handling are oriented to business continuity and disaster recovery. As a result, a proper root cause analysis is often overlooked.

$18.3 MILLION

Annual cost of **CYBERATTACKS** by banking industry

Source: The Cost of Cybercrime, conducted by Poneman Institute LLC

Many organizations face difficulties in gathering sufficient quality evidence for a comprehensive investigation to be carried out when an incident happens.

RESPONDENTS do not have formal cyber resilience plan in their organization

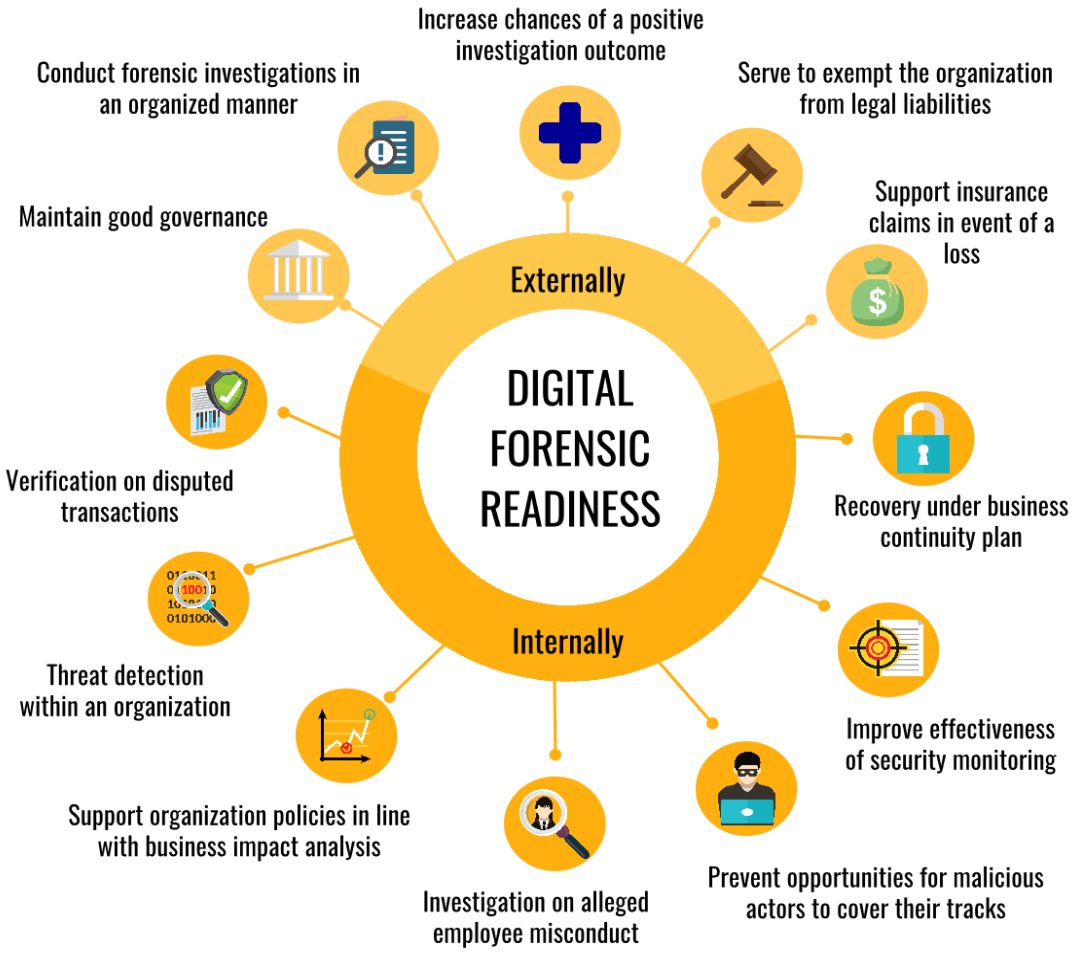
Source: IBM study more than half of organizations with cybersecurity incident response plans fail to test them

Digital forensic readiness can be described as an organization's capability to collect, preserve, and analyze digital evidence.

The objective is to maximize the potential in using digital evidence while minimizing the cost and time required for an investigation.

In other words, it is the condition of being prepared in such a way that digital evidence is appropriately acquired before an incident so that it can be readily available when the need arises without interrupting business operations.

By adopting digital forensic readiness, organizations can leverage this for both external and internal purposes.



In essence, the planning for digital forensic readiness requires identification and assessment of risk areas within an organization and actions to be taken to avoid and minimize the impact of the identified risks.

It should also involve a comprehensive review and analysis of an organization's current security posture, which covers implemented technical controls, policies, procedures, and employee skillset.

Today, increased dependency on information technology for business operations has resulted in the creation of digital footprints which can be used to unravel the specifics of an unexpected incident.

Organizations should shift their focus from reactively approaching incidents to being proactively prepared even before incidents are likely to occur to maximize the potential of investigations that will yield positive outcomes while minimizing time and cost.

REFERENCES

https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf

https://www.bcg.com/d/press/20june2019-global-wealth-report-222692

https://newsroom.ibm.com/2019-04-11-IBM-Study-More-Than-Half-of-Organizations-with-Cybersecurity-Incident-Response-Plans-Fail-to-Test-Them

https://www.isaca.org/resources/isaca-journal/past-issues/2014/importance-of-forensic-readiness

https://digital-forensics.enterprisesecuritymag.com/cxoinsight/digital-forensic-readiness-planning-and-readiness-checklist-in-order-to-reduce-business-risk-nid-1184-cid-59.html

https://www.nationalarchives.gov.uk/documents/information-management/forensic-readiness.pdf

https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B13342-B4E0-1F6A-156F501C49CF5F51.pdf

https://pub.rebit.org.in/inline-files/DigitalForensicReadinessChecklist.pdf