10 STEP

CYBER INCIDENT RESPONSE PLAN

10 STEPS FOR

ARMING YOURSELF IN CYBER WARFARE

1. Assign an executive to take on responsibility for an incident response plan (IRP) and for integrating efforts across business units and geographies.

2. Identify the key individuals who are necessary for the IRP and ensure redundancy. Representation should come from Executive, Legal, Finance, Information Technology. Human Resources and Risk.

3. Develop a register of risks, threats, and potential failure modes. Refresh them quarterly on the basis of changes in operations and threat environment.

4. Develop easily accessible quick-response guides for likely scenarios and escalation procedures.

5. Maintain relationships with key external stakeholders, such as law enforcement.

6. Maintain service-level agreements and relationships with external breach-remediation providers and experts (for example, Legal Counsel, Forensic Investigators, Public Relations). Make certain contacts from those providers are contemplated within the IRP. If you purchase Cyber insurance, review the list of panel service providers and make the same arrangements.

7. Ensure that documentation of the IRP is easily accessible to all team members.

8. Train, practice, and run simulated breaches in the form of tabletop exercises. The best-prepared organizations routinely conduct war games to stress-test their plans, increasing managers' awareness and fine-tuning their response capabilities.

9. Secure all logs, audits, notes, documentation and any other evidence that was gathered during the incident with appropriate identification marks, securing the chain of custody for future prosecution and insurance claims.

10. Document the time in man-hours (internal and external), as well as the cost of handling the incident/remediation.

Employees remain the greatest area of concern for cyber incidents, whether via willful acts or negligence. Significant risk arises specifically from employees who are the target of social engineering scams.

Source: Harvard Business Review

> **"EVERY ORGANIZATION…IS AT RISK OF HAVING ITS PERIMETER BREACHED AND ITS CRITICAL ASSETS COMPROMISED."**
>
> *– McKinsey and Co*

CYBER
GOING MAINSTREAM

CYBER RISK CRIMINALS ARE BECOMING MORE SOPHISTICATED, BUT THEIR OLD TRICKS CONTINUE TO WORK.

A recent report from Dtex systems uncovered the alarming fact that in 95 percent of their assessments, employees were "researching, installing or executing security or vulnerability testing tools in attempts to bypass corporate security."

THE DTEX REPORT HIGHLIGHT

TWO KEY AREAS THAT ARE DRIVING CYBER-RELATED RISK:

PEOPLE

68% OF ALL INSIDER BREACHES ARE DUE TO NEGLIGENCE

22% ARE MALICIOUS INSIDERS
First two and last two weeks of employment are high-risk timeframes

10% ARE RELATED TO CREDENTIAL THEFT

CLOUD SYSTEM

64%

of companies assessed **HAD PRIVATE CORPORATE INFORMATION PUBLICLY AVAILABLE** on the web due to employees' improper use of cloud storage services.

ACCORDING TO DATA BREACH INVESTIGATIONS REPORT BY verizon

- **81%** OF HACKING-RELATED BREACHES LEVERAGED STOLEN AND/OR WEAK PASSWORDS
- **7%** OF PEOPLE STILL FALL FOR PHISHING EMAILS OR SCAMS
- **73%** OF BREACHES WERE FINANCIALLY MOTIVATED
- **51%** INVOLVED ORGANIZED CRIMINAL GROUPS