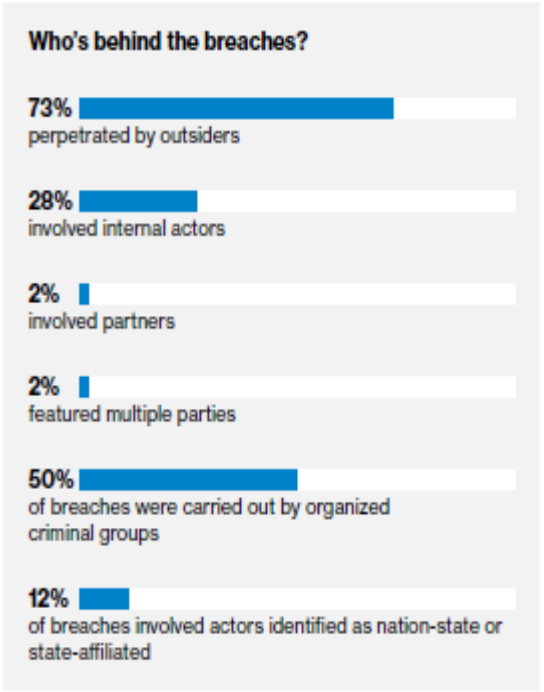
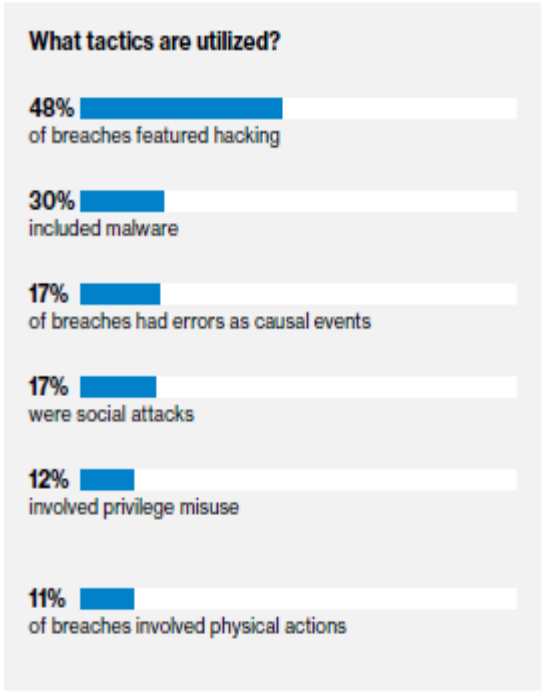
Building Cyber resilience to prepare for cyber-attacks and data breaches

Presented By: Meetali Sharma

Snapshot from Verizon report





Source: Verizon - 2018 Data Breach Investigations Report

2

Cyber Security Vs Cyber resilience

Cyber Security

- Cyber security consists of technologies, processes and measures that are designed to protect systems, networks and data from cyber crimes.
- Effective cyber security reduces the risk of a cyber attack and protects entities, organizations and individuals from the deliberate exploitation of systems, networks and technologies

Cyber Resilience

- Cyber resilience looks at a wider scope where it comprises cyber security and business resilience.
- Cyber resilience helps businesses to recognize that hackers have the advantage of innovative tools, element of surprise, target and can be successful in their attempt. This concept helps business to prepare, prevent, respond and successfully recover to the intended secure state.
- In comparison to cyber security, cyber resilience requires the business to think differently and be more agile on handling attacks.

Steps towards Cyber resilience - Identify

- **Conduct Risk Assessment of current environment to identify** -
  - ✓ Threat Landscape
  - ✓ Existing Controls
  - ✓ Security Posture
  - ✓ Business Goals
  - ✓ Regular Risk Assessments and controls optimization to build threat resilience

- **Understand your environment** -
  - ✓ Where is the data created, collected and stored
  - ✓ What is the current network infrastructure
  - ✓ Inventory of assets (systems & software)

4

Steps towards Cyber resilience – Plan & Protect

- **Perform Vulnerability and Penetration Testing**
  - ✓ Once you have the necessary security systems in place, it is equally important to test it from time to time to find out its efficiency and strength. You should perform vulnerability and penetration testing on your security systems regularly – monthly or a quarterly basis

- **Maintain Up-to-Date Software**
  - ✓ One of the primary things that you can do to protect yourself and your organization from cyber attacks is to stay up-to-date on the software you use – maintain up to date patches and critical software updates

- **Proper Backups**:
  - ✓ Back-up all your critical data, files. Maintaining back-ups diligently will help you retain and retrieve crucial information in the event of a cyber attack.

5

Steps towards Cyber resilience – Plan & Protect

- **Email protection**
  - ✓ Emails have become one of the primary targets of cyber attacks, the main communication tool in organizations, both internally and externally. Host anti-spam and/or e-mail services that will help protect your business.
- **Manage User Privileges and Access Rights**
  - ✓ Control and limit the users' administrative capabilities for systems and social footprints.

- **Implement preventive controls based on results of risk assessment**
  - ✓ These include, but not limited to, laptops encryption, admin rights blocking for users, exe blocking and restricted folder sharing within the network, USB ports blocked at end points, server monitoring, logs monitoring through SIEM, High privileged accounts monitoring, anti-virus updation and monitoring, vulnerability management on a monthly basis along with tracking of patches deployment through SCCM, employee awareness & training along with regular spot checks and internal audits, continuous monitoring through metrics and internal GRC/IRM tool, network segregation based on customer/project/internal business needs. All these controls can help us stay protected against all the ransomware and malware attacks

6

Steps towards Cyber resilience – Employee Training

- ✓ Regular training of personnel - conduct annual or bi-annual training in security practices that can help your employees understand acceptable security practices, user security policies, and various tips to prevent security breaches.
- ✓ Explain how to protect laptops, mobile devices, and digital storage media.
- ✓ Monitoring of activities – Run phishing and simulation drills
- ✓ Encourage employees to report suspicious activity
- ✓ Conduct background checks
- ✓ It is imperative that everyone in the organization – right from the new hire to the top management – understands the need to take security seriously and feels responsible and accountable for maintaining security.

7

Steps towards Cyber resilience – Detect

- **Establish basic levels of software such as**:
  - ✓ **Encryption Software**: This software can help encrypt and protect all your sensitive data such as customer information, financial statements, employee records, and client information.
  - ✓ **Data Backup Solutions**: Data Backup Solutions can help backup all your business-critical data. In the event of any information loss or compromise, you can quickly retrieve the data from the alternate backup location.
  - ✓ **Password Security Software**: With a password security software, you can set up a two-step authentication or password security for your internal programs to reduce the probability of hacking of passwords.
  - ✓ **Antivirus Software**: An antivirus software can be your primary defense against most types of malware.
  - ✓ **Firewalls**: Firewalls can help provide an added layer of protection to any hardware or software. Firewalls can help prevent an unauthorized user from accessing a computer or network.

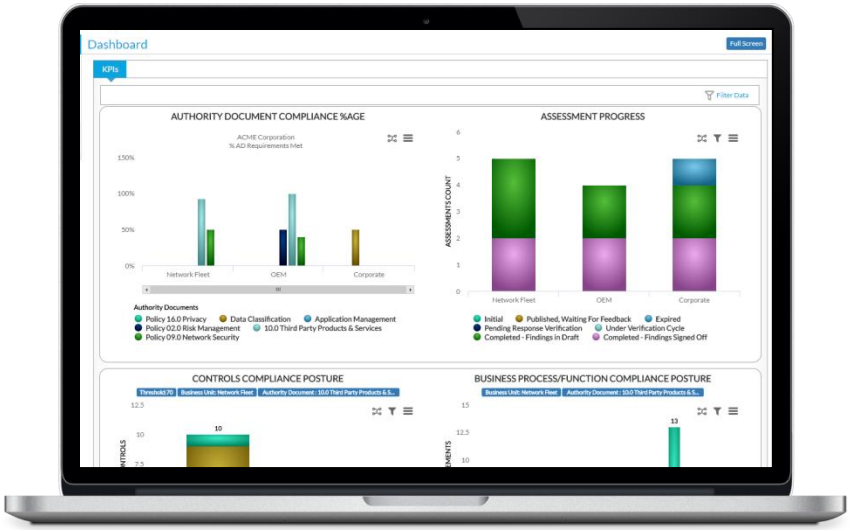
8

Steps towards Cyber resilience – Detect

GRC Tool implementation

Steps towards Cyber resilience – Detect

TruOps™ offers seamless integration of risk management program across functions, such as IT operations, security operations, compliance, DR/BCP, vendor risk management, governance & audit.



GRC Tool implementation

TruOps

- SecDevOps
- IT Risk
- IT Compliance
- Business Continuity Management
- Vendor Risk Management
- Issue & Exception Management
- IT Policy

Connecting Cybersecurity Risks to GRC

- Identity Risk Management
- Security Risk Management
- Application Risk Management

Steps towards Cyber resilience – Respond

- **Have a well defined Incident Response Plan**
  - ✓ Emails The incident response plan should provide a framework for action so that important decisions have been considered ahead of time and are not made under pressure. In particular, it is important for the incident response plan to provide procedures and guidelines on difficult issues, including identifying lines of authority and internal reporting obligations.
  - ✓ Once you have an incident response plan in place, it is important to test it regularly—annually, if possible. These “tabletop” exercises should involve the full incident response team, and the results of the exercise should be made available to senior management.

- **Have a Proper Resiliency Plan**
  - ✓ This plan should have properly laid out protocols that employees can follow to manage a situation when a breach occurs. You should also regularly conduct mock drills to test the efficacy of your resilience plan and to fine-tune it, if necessary. Such mock drills will also help your employees gain hands-on practice as well as confidence in being able to detect quickly and contain a breach, if and when it occurs.

Steps towards Cyber resilience – Few considerations

- **Management Involvement**
  - ✓ You should gain leadership buy-in through executive and board engagement to make your security culture all-inclusive. Such a leadership involvement towards cyber resilience is crucial, as it helps deliver a strong message to employees, vendors, and partners about the organization's commitment to fighting cyber attacks and cyber crimes.

- **Holistic Approach**
  - ✓ Implement company-wide security policies that will help reduce the likelihood of an attack. Everyone must be made responsible and accountable for cyber security.

- **Have a Proper Insurance Plan**
  - ✓ Once a business or organization knows its systems and data and understands its exposures, it will be well-positioned to work with an independent insurance agent or broker to evaluate its cyber insurance needs and to obtain coverage in this fast-growing insurance market

12

Even well prepared companies may not know immediately that they have been breached. But those that have prepared for such an event will be much better off than those that have not. Just as conducting fire drills can save lives in the event of a real fire, preparing for the aftermath of a cyber attack can make an enormous difference in how quickly your company gets back on its feet after a major breach

Cyber strategies should be focused not simply on identifying individual risks, but on developing resilience and protection as a key focus.

The goal should be to develop resilience and protection, because as cyber risks accumulate it becomes more difficult to anticipate them all

Stay Secured, Protected & Resilient

13

THANK YOU

Contact Details –

Meetali Sharma
meetalisharma81@gmail.com;
meetali.arora@sdgc.com
+91-9971393639