Security Protection Principles
Volume 1 Edition 2

CVEEM Consulting Group

Comprehensive Security Policies and ITIL Operations hygiene is the best way to protect the Enterprise.

Your Company is at risk using only cybersecurity protections to keep hackers out. Track your documents in your network with data loss (DLP) software.

Organizations today exist in a complex and interconnected digital ecosystem. Sharing data and information with customers and vendors electronically is here now more than ever before.

Companies must understand 3rd party relationships and employee access to company data to manage and understand the risk of digital operations to determine where your enterprise is most vulnerable. You need to know who has access to what data and where the information is going.

Security protection from unwanted hacker access must be in balance with other vulnerability sources. Security protections are paramount for your long term success. I have spent 20 years in secure digital operations and SaaS infrastructure and I can help you produce a scalable security capability.

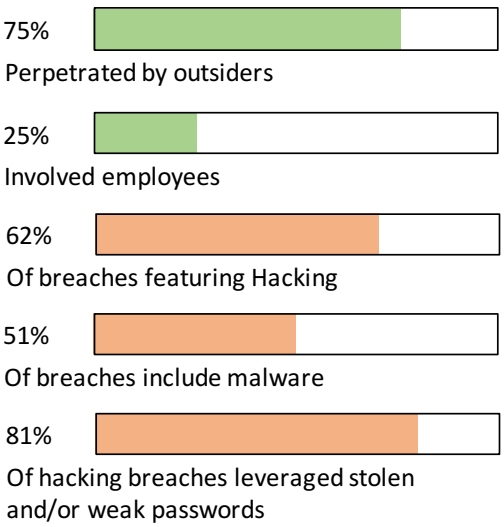
Threats and the Value of Security

In 2017, according to Verizon breach records, there were 42,068 security incidents with the number of actual breaches with data loss to be 1,935. Employee notification was the most common internal discovery method indicating that awareness programs can be effective.

The policy to keep intruders from entering the corporate security envelope will never be 100% effective. You will have a data breach statistically a phishing email breach.

Risk assessment and data classification of information, security policies and practices for IT operations and monitoring of outbound / internetwork traffic with data loss protection software are the best methods to reduce vulnerabilities and hence security risks.

Summary Breach Details 2017



Source: 2017 Data Breach Report, Verizon, 2017

After effective perimeter security is functional, the ROI for an additional $1 is best deployed to monitor and track company data inside the enterprise.

Craig Shrader,
Managing Director
CVEEM Consulting Group

What You should be Doing

- Enforce operations digital hygiene including firewalls and methods for external protection.
- Maintain Security/OS patches in PCs & infrastructure systems.
- Two factor authentication for User logins.
- Backup PC and servers. Enforce backup policies.
- Monitor document files within enterprise network.

How CVEEM Can Assist YOU

- Review of Policy & Practices and Make Remedies
- Develop and Implement Risk Assessment
- Improve/Modify Operational Practices for Users & IT.
- Conduct Audit & Remedies for Compliance Certification
- Develop / Enhance Security Training and Awareness
- Assessment of Security Team Recommend Change
- Develop / Enhance Security Documentation

Corporate User Awareness

Education and Security Awareness is the best way to reduce risks from end-point breaches from phishing email and malware.

CVEEM Consulting Group
Craig Shrader, Managing Director
908 568 1532 I cccornell.shrader@gmail.com