Vulnerabilities

Impacts

Impacts are the resulting effects of a risk that is realized. Impacts are the items that an organization is attempting to avoid with a security incident.

Data Related

Data Loss

Data loss is when an organization actually loses information.

Files can be deleted, overwritten, or even misplaced.

Data Breaches

Data breaches are the release of data to unauthorized parties.

Having a data breach can be a legal issue, a financial issue, a reputation issue, or any combination of these issues, depending on the type and scope of the breach.

Data Exfiltration

Data exfiltration is the exporting of stolen data from an enterprise.

Data exfiltration impact is related to the data being stolen.

Identity Theft

Identity theft is a crime where someone uses information on another party to impersonate them.

This is a secondary impact once data is exfiltrated.

The impact of data exfiltration that includes personally identifiable information (PII) can be significant in terms of regulatory costs

Financial

At the end of the day, risk is measured in financial terms, and the impact from vulnerabilities can be expressed in financial terms as well.

- Costs associated with investigating and fixing enterprise systems
- Lost orders/revenue due to system downtime
- Fines for regulatory noncompliance on privacy laws
- Attorney fees from lawsuits
- Ransom payments made for ransomware
- Losses due to stolen intellectual property
- Share price decline and market capitalization loss

List of items that can contribute to the financial cost

Reputation

Reputation impact as a result of a cyber attack comes in two main forms: loss of customer confidence and, in cases where skilled workforce is involved, a competitive field loss of key employees.

Availability Loss

Availability is defined as resources being available for authorized users when they are supposed to be available.

Improper or Weak Patch Management

All systems need patches periodically as errors and vulnerabilities are discovered and vendors issue software fixes to these vulnerabilities.

One of the important takeaways from patching is that once a supplier patches their software, hackers can reverse engineer the vulnerability from the patch.

To manage the risk associated with patch management vulnerabilities, it is important to establish a strong patch management program that covers all systems and all software.

Because patches can be time sensitive, it is important to have defined periods of time when patches must be installed as well as an automated means of determining what patches are needed, where they are needed, and status of the current patch level by target location.

Firmware

Firmware is just another form of software with one noted distinction: it is stored in hardware to be present when the system boots up.

With firmware being part of the system itself, always present, it is frequently missed when considering how to keep software up to date.

The lifecycle, vulnerabilities, and maintenance issues associated with firmware mirror those of software.

Operating System (OS)

Today, major operating systems can patch themselves, and with a little automation, the tracking and management of patches is easy.

There are only a couple of steps to get this right.

First, have a patch management policy, and make it patch everything and track all patches.

Second, follow up on that policy.

Applications

Applications are the programs that comprise the functional aspect of the enterprise.

The challenge with application patching across an enterprise is in the tracking of all of the applications used, including even small, seemingly meaningless programs that are installed on desktops.

Not only does the enterprise have to keep track of all the applications it has, but it has to determine which ones have updates and when.

Third-Party Risks

Supply Chain

The enterprise computing environment is full of third parties, and their risks become enterprise risks.

Vendor Management

A vendor or supplier is a firm that has a business relationship with the enterprise.

The challenge of vendor management is one of determining one's own needs and then finding the vendors that offer the best value proposition against those needs.

For most components in an enterprise; issues of support, system lifetime, and maintenance all play a role in the long term value of a vendor and their products.

System Integration

Enterprises are composed of many different components that all work together to process the information that flows through the enterprise.

System integration is the connecting of these components, each representing a portion of the system into a complete functioning unit.

System integration is an area where vulnerabilities can exist, as the pieces can have gaps in their integration or capabilities that do not manifest per the desired specification.

System integration is coupled with configuration management because the configurations of the individual pieces can affect how the system as a whole functions.

Lack of Vendor Support

When an item reaches its end of life (EOL) from the original manufacturer's standpoint, this signifies the finality of its life under almost all circumstances.

After the manufacturer stops supporting an item, options to keep it up to date with patches and fixes seldom exist. At this point, an organization that continues to use the product assumes all of the risk associated with issues uncovered after the product has entered EOL status

Another scenario in which lack of vendor support arises is when the system in question is implemented by a third-party vendor and that vendor either no longer supports the configuration or is no longer in business.

The underlying technology may still be supported by the original manufacturers, but the lack of support for the middleware provided by the third-party implementer raises questions as to whether the underlying products can be updated or patched.

Outsources Code Development

Code can be one of the greatest sources of vulnerabilities and risk in an enterprise.

The risk isn't just in the fact that the code is outsourced, but actually in the fact that the visibility and control over these risks becomes harder to manage with every step away from the source.

It is important to have conditions in contracts requiring appropriate development measures be in place for third-party code, including the rights to inspect and verify security functionality.

Ensuring third-party developers have appropriately secure coding practices and having their code reviewed by independent testers and placed in escrow for safekeeping are considered best practices.

Data Storage

If all data was in a single location, then data storage management, including backup and recovery functions, would be easy to manage.

Ensuring the correct access controls and security protections, such as backups, is important for all data stores, and when gaps in these controls emerge, this creates vulnerabilities.

To ensure all data is protected from becoming a vulnerability to the system, having a standardized data storage policy and checklist is good practice in the enterprise.

Legacy Platforms

Legacy platforms is the term used to describe systems that are no longer being marketed or supported.

Legacy systems represent an interesting vulnerability because, by being in the legacy category, they are no longer supported, so if new problems are discovered, the only fix is a compensating control.

Exam Tips

Unchecked vulnerabilities due to weak configurations, third party risks, improper/weak patch management, and legacy platforms can result in major impacts, including data loss, breaches, exfiltration, and identity theft, as well as financial, reputational, and availability loss.

Part of a security professional's responsibilities is to keep up with current Common Vulnerabilities and Exposures (CVEs) and update or patch systems to keep the enterprise environment secure. This applies to firmware, operating systems, applications, virtual machines, and devices.

Updates and patching are used to ensure software and firmware are up to date and secure. Manufacturers of hardware often provide updates for firmware, and it is the organization's responsibility to ensure firmware updates are applied.

Supply chain concerns and lack of vendor support are concerns directly related to third-party risks and management.

Do not be confused! End of life (EOL) is the term used to denote that something has reached the end of its "useful life." End of service life (EOSL) or end of support is when the manufacturer quits selling an item. In most cases, the manufacturer no longer provides maintenance services or updates.

A system can have vulnerabilities related to its age. Whether the system is composed of old parts, as in an embedded system, or has become an end-of-life legacy system, the lack of vendor support can result in the owner's inability to address many newly discovered issues.