Managing IT Risk in the Life Sciences Industry:

What You Should Know About Biotech Companies' IT Infrastructure

The life sciences industry is extremely data-driven, with companies constantly monitoring their experiments for the slightest change in results. IT is critical to their success, which means any risk to their infrastructure is extremely risky. The failure of a single device or software update could shut down an entire research facility until the problem is resolved. Because these risks are so high, many biotechnology companies implement strict security measures and maintenance procedures to protect their IT infrastructure. Read on to learn more about IT risk in the life sciences industry and what you can do to mitigate your own risks as an IT professional working with biotech customers.

What is IT Risk in the Life Sciences Industry?

IT risk is the risk to business operations due to the failure of IT systems and processes. Life sciences companies have specific risks due to their industry that must be managed carefully. The inability to access data due to a cyber-attack or data breach is a major risk, as well as the potential for a system failure to affect a large number of users. IT risk may also include potential legal or compliance issues, such as improperly disposing of electronic waste. When managed effectively, IT risk helps companies remain agile and profitable. When significant risks go unmanaged, however, businesses can be significantly impacted. When managing IT risk in the life sciences industry, it is important to keep in mind the sensitive data these companies handle. For example, genomic data is very sensitive. Inadequate security measures could lead to the loss of this data, which could result in a major PR disaster and loss of customers, as well as regulatory fines.

Maintaining an Effective IT Infrastructure in the Life Sciences Industry

Many life sciences companies have strict maintenance windows for their networks, devices, and other infrastructure. Downtime is costly, so IT teams need to be extremely careful when making updates to ensure the entire network is not impacted. This may include shutting down certain portions of the network, such as a segment of a local area network or network segment, or shutting down entire systems. With proper planning, work with the business to determine which devices or systems should be shut down and when, and the use of appropriate change management procedures, IT teams can successfully complete necessary updates and keep the business operating smoothly. Another important maintenance task is device inventory management. Biotech companies often use multiple vendors to provide networking and other infrastructure services. Having a centralized inventory of these devices and systems makes it easy to coordinate maintenance and keep track of change requests. Network device inventory management software can help you with this effort.

Why is Network Security Important for the Life Sciences Industry?

Biotech companies typically handle extremely sensitive information, such as genomic data. This data must remain private and secure, so network security is critical. Network security is also important to protect the integrity of data and prevent data loss due to network-based threats such as viruses or other malware. Network security may include firewalls, network intrusion detection systems, or network intrusion prevention systems. Network security may also include virtual private network (VPN) connections to protect data in transit between a remote user and the company's network. This may include using the Internet to connect remotely to a company network. In some cases, the company may use a private WAN to connect to remote users.

Protecting Network Infrastructure with Biometric Access Controls

Biotech companies dealing with sensitive information may implement network access controls, such as biometric authentication. These authentication methods use unique biological features, such as fingerprints, hand geometry, facial recognition, or iris/retina scanning, to verify a person's identity. This helps ensure only authorized individuals have access to sensitive data. Some companies may choose to use biometrics on both the network and the endpoint level, such as laptops or computers. Network access control systems provide a centralized management console that can be used to provision user access to the network, as well as monitor and audit access to the network. This centralized console can also be used to manage network infrastructure devices, such as network switches and routers. This ensures only authorized users have access to network infrastructure devices.

Limiting Device Exposure with Visibility and Control Over Software Changes

Some industries, such as life sciences, require strict visibility and control over software changes. This includes tracking any changes to software installed on critical devices. This visibility and control over software changes can help mitigate the risk of failed patches or software updates causing a critical device to cease functioning. This visibility and control over software changes can also be used to track any unauthorized software changes on critical devices. If a device unexpectedly changes, such as a switch or router, it may indicate malware or malicious activity on that device.

Backup and Recovery Strategies for Network Equipment Rooms

A network equipment room or NER houses network switches, routers, firewalls, and other critical network infrastructure devices. It is important to maintain a reliable backup and recovery strategy for these devices. This may include using on-site generators and uninterruptible power supply (UPS) systems, storing backup devices in a secure off-site location, or using cloud-based solutions for backup and recovery. When storing backup devices in an on-site location, make sure this room is properly secured, such as using a metal cabinet to protect the devices from environmental exposure. If storing backup devices off-site, make sure they are encrypted and regularly transported to an off-site location.

Conclusion

The life sciences industry is extremely data-driven, meaning any risk to their IT infrastructure is extremely risky. It isn't uncommon for biotech companies to shut down their entire research facility until the problem is resolved. Managing this risk often involves strict security measures and maintenance procedures to protect their IT infrastructure.