CRITICAL DATA AND DEVICE PROTECTION

Now more than ever, it's essential that your technology provider understands the importance of keeping your devices and data secure.

You should choose a provider who has the tools to handle the physical security of your assets and the data contained in each of those assets. Your provider should be equipped with powerful servers and a robust infrastructure behind it all. There's a lot on the line. Your confidential data, finances, projects, customer relationships, and privacy should be just as important to your provider as it is to you.

The average loss per data breach last year:

$8.94 million

-Ponemon

HERE ARE 10 WAYS YOUR TECHNOLOGY PROVIDER CAN HELP PROTECT YOUR DATA AND DEVICES

1 Surveillance

Security personnel on-premise is important. It's even better when the personnel are on site, whether daily or extended 24/7. This helps to make sure your expensive assets are looked after. Metal detectors at each entrance can also help as they can deter individuals from the temptation of theft.

2 Enforced Visitor Policies

Entry to the facility that is storing your valuable devices and data should have careful controls over who can visit and when. A visitor sign-in log maintains visibility into who has entered the building and when. Visitor escorts provide a means to account for each visitor. Policies should be established to account for truck drivers and third-party vendors as well. For example, at CompuCom we have designated loading parameters where truck drivers are only permitted to access. We also do not accept non-scheduled deliveries.

3 Controlled Access

Just as access to employees' email accounts and shared company drives is controlled, a provider should apply the same standards physically at facilities. You don't want just anyone to be able to access your networks, only those who have special outlined permission to. We require limited key-card access and keep every customer's assets segregated.

4 Inventory Management

Your provider should make sure all assets in their facility are accounted for. At our facilities, we don't just check every quarter, but monthly. We perform a monthly cycle count of all products, and we're proud to have historical variances less than .01%. Ask your provider how often they check their inventory, and throw them a curve ball by asking what their variances have been.

CompuCom®

5 Data Asset Containment

Providers must consider customer assets, especially data, as proprietary or confidential. Nothing should be shared. This means that photography, employee mobile devices, and USB removable media should be restricted or prohibited. We understand the importance of our customers' privacy, and we enforce strict policies to maintain this.

6 Careful Network Protection

Network exposure is risky, and therefore each network needs to be carefully handled. This means using encrypted domains for VPN connections, physical isolation of each network, and following granular firewall rules. We physically segregate each of our customer's networks in a secured server room, each in a customer-specific server cabinet. Dedicated fiber flows the data from the server room to our configuration benches, eliminating the use of VLANs. Networks should not be routed on the same wire. Quiz your provider about how they handle and protect their network, and encourage them to get specific.

7 Strict Employee Policies

Visitors are not the only ones that should have strict rules while in your provider's facility. Associates, contractors, and any personnel that work in or enter the facility should be aware of, and follow, stringent policies while on site. A policy example could be prohibiting employees from using their mobile devices or taking photography footage of facility areas that contain customer assets. A way that this can be enforced is through conducting employee bag inspections upon entry.

8 Continuous Training and Education

Orientation and training typically takes place when employees are onboarded in any given organization, but when it comes to a role where they are working with sensitive customer assets, a standard onboarding is simply not enough. Employees must be made aware of each customers' specific security policies. They must also be kept up to date as these customer policies change. CompuCom requires our employees to complete orientation and training that includes a policy review of each of our customers' confidentiality, safety, and security procedures. We also require annual training so that our employees always remain well-informed with our latest security standards.

9 Certification Upkeep

Technology providers have no legitimate excuse not to be kept current with the latest security standards. There are well-known, internationally recognized industry standards that customers can, or at least should, expect their providers to meet (e.g., ISO/IEC 27000 and NIST). Again, that's why we require annual employee training. We also require annual policy recertifications to maintain compliance with the latest international standards.

10 Transparency

Above all else, your technology provider should be transparent with you. You're trusting your provider with a lot, and they owe it to you to keep you honestly and consistently informed. We actually welcome our customers to send us security questionnaires, visit our facility, and perform third-party audits. That's because we're confident in the security measures and policies that we uphold. Are you that confident in your provider?

ENHANCE YOUR SECURITY

There are bad actors just waiting and looking for ways to exploit your information, and if your provider isn't maintaining the highest standards for the security of your assets—your physical devices and your networks and data—you might as well consider your provider to be one of those bad actors too. Your provider should have your back—always.

We're committed to more than providing data security to our customers. We're committed to excellence. Our comprehensive approach to information security and risk mitigation includes vigorously protecting our customers' privacy, confidential data, and personally identifiable information. With us, you can have peace of mind and be at ease knowing that your business is thoughtfully protected.

Learn more about CompuCom and our vision for connecting people, technology, and the edge with a seamless experience at <u>compucom.com</u> or call us at 1-800-350-8430.