## COMPLIANCE CAN HURT BUT IT DOESN'T HAVE TO

Following best practices is a commitment at the best of times. but when you don't have the specter of industry and government compliance hanging over you, it can say a great deal about how you operate. The organizations that are committed to staying in business for the long haul understood early on that good practice is about continuous improvement and should be ingrained in company culture and behaviors from the outset. They add it as an extra layer of security towards their longevity but that does not mean doing things right cannot cause a headache. Compliance is hard work not least because it places a time span and therefore pressure on everything. It is very evident in data circles where the biggest boom has occurred.

Once upon a time data compliance meant fulfilling national legislation obligation around security, today the sheer overwhelming amounts of data being generated by businesses has seen this view turn into a global one as GDPR has come into effect. So which compliance requirements are causing pain?

**GDPR**

The General Data Protection Regulation (GDPR) took effect on May 25, 2018. This all pervading EU legislation looks at how an organization uses, handles and safeguards its data in respect to the individual's privacy. It does not stop there as it casts it's beady eye over any affiliations through third party vendors too. Any organization dealing with European goods or services and therefore associated data for customers of any kind will need to comply with GDPR. Data inventory, data mapping, consent/opt ins for use of personal data, respecting an individual's 'right to be forgotten,' and auditing are some things to expect. Non compliance will result in fines of up to 4% global turnover.

**Patch management/software updates**

IT leaders have to be extra vigilant about their security protocols. Forgetting about lapsed patches and software updates is tantamount to leaving a door wide open to attack. Unnecessary risks come from this most basic oversight as many businesses have discovered especially when it comes to third party vendors. The challenge facing IT departments is the deluge of patches, unfortunately there is no easy answer to this other than to stay on top of it with a regular patch management strategy. In this way vulnerabilities are not exposed and exploited.

**BYOD**

Bring your own devices (BYOD) options have blossomed into a new interconnected way of life as employees can use them to connect to work systems. Although there are many advantages IT leaders must also be aware of the threat they can present. Smartphones and tablets bring security vulnerabilities right into the workplace.

Organizations can mitigate this issue through a strong bring-your-own-device policy backed up by technical controls. Mobile device management protocols, such as Google Mobile Device Management, are key to oversight in this area because they provide the ability to remotely remove access to selected accounts or wipe a device.

Furthermore, managers can prevent critical data from being compromised, whether stolen, or simply lost, by enforcing device lock passwords. And adhering to the ISO recommendations, SMS should be replaced with a time-based one-time password-based method, such as Google Authenticator.

- Outlining a clear approval process for devices. BYOD doesn't mean employees can just start using their personal devices for business tasks right away. Certain precautions must be taken
- Leadership must account for for multiple mobile device types. And these devices can range across a larger scope of supported devices than normal
- Setting and enforcing strong passwords
- Having a plan for lost or stolen mobile devices
- Rollout of a complete MDM (Mobile Device Management) solution

**EDI/vendor management**

A chain is only as strong as it's weakest link. A major vulnerability point that plagues many companies comes from Electronic Data Interchanges (EDI), and vendor integrations. Soha Systems published a report in 2017 that indicated that as many as 63 percent of all reported data breaches originated directly or indirectly from third party vendors. Many of the most heavily publicized data breaches, from Target (HVAC) to Home Depot (POS software on handheld devices) to Philips (payroll processor), have originated as breaches at a third-party vendor. Managing not only vendor information security but also vendor compliance with privacy laws is a major undertaking and significant compliance challenge.

**IoT**

As more and more devices, from phones to lightbulbs to doorbells have become internet enabled and connected, the Internet of Things (IoT) has led to an explosive growth in the number of endpoints and devices that could also introduce potential security holes to a system, network , or business. IoT security standards have lagged badly, creating a potentially huge number of new vulnerabilities in organizations' networks. This digital-physical convergence is being seen across almost all industries, including financial services, automotive, retail, food and beverage, industrial, energy, oil and gas, transportation and utilities companies. Unlike some other threats to an organization's network, IoT endpoint vulnerabilities could ultimately lead to more than financial or reputational harm, but actual physical harm to individuals as well as systems. One method of ensuring security within IoT subsystems is by carrying out penetration tests.

Many regulations including SOC2 require an external penetration test annually at minimum, and best practices often involve both externally run and internally controlled tests being performed at a far more frequent basis. Targeting IoT infrastructure end points should also be a part of these tests. With the increase of the number of qualified and competent security vendors, enabling penetration tests as a regular part of business is fast become a Standard Operating Procedure for businesses looking to remain relevant for many years to come.

Another technique that is ultimately very effective, is the sandboxing of IoT devices into a separate area of a companies network. Responsible companies will often segment their networks into many slices, keeping development, testing and production areas completely distinct and separate. Taking this method one step further, adding segments for guest access, as well as BYOD and IoT devices will keep the risks of allowing for these policies to be minimized.

The fast pace of growth in assorted areas within the technology realm makes sticking to the assorted requirements of compliance a challenging, but fruitful task. sacrificing a small amount of speed for a great deal of security is almost always the right call. Compliance can be a painful thing in the short term, but embracing it at the beginning of a product, process or business venture will make all the difference in the long run.