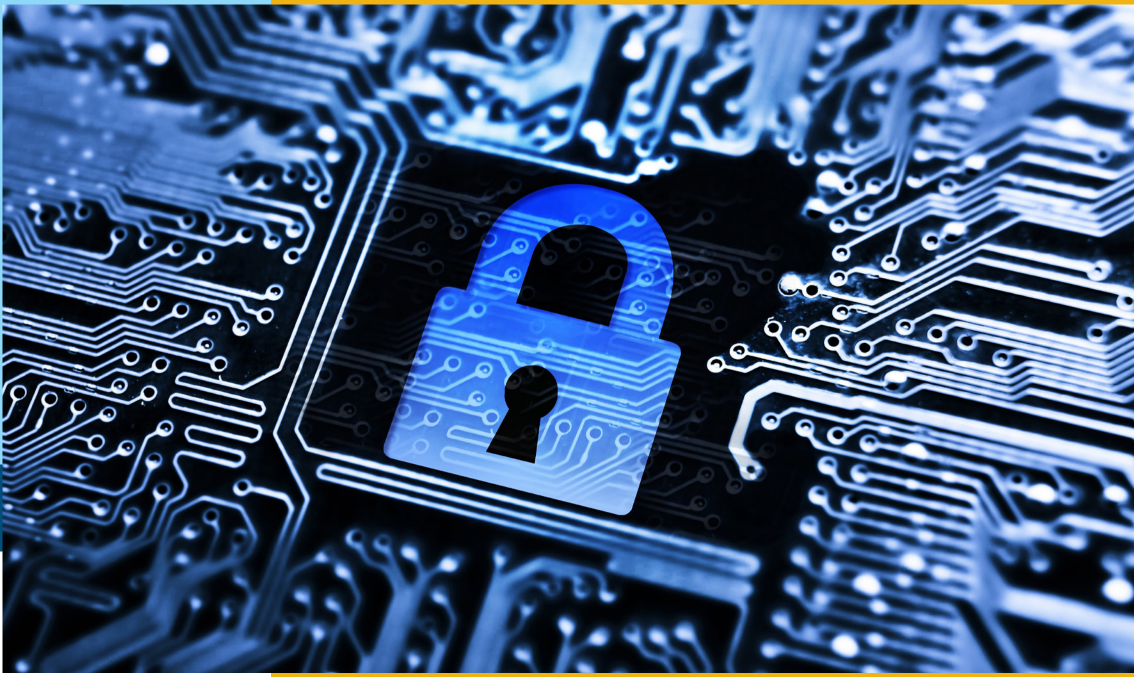
TEN STEPS TO ADDRESS SECURITY



Intivix.com

(415) 543 1033

TEN STEPS TO ADDRESS SECURITY RISK

Awareness

We live in an ever changing world with major crisis that are no longer isolating themselves. These threats include the terror inflicted in physical harm, political controversies, and religious fanaticism trying to weaken our economy. However, there is another war out there: a constant battle against cybercrime trying break our economy. Large corporations are no longer the only targets. Ransomware is being used for financial gain, climbing to $1.1 million in 2014 through bitcoins; according to symantec report on “The Evolution of Ransomware” from August 2016, resulting in losses amounting to 18 million dollars in 2015 for business owners.

Organized crime and terrorist organizations look for means to finance and keep pushing their agenda and idealisms forward and cybercrime has become an easy way to obtain money while keeping their anonymity.

What is at Stake?

It’s not only your business information at stake but your customers secure information such as social security numbers, credit card information, or any other private information stored in your servers and network is at risk as well. Ultimately, when your clients give you secure information, you are responsible on how that information is managed and protected.

The “California Security Breach Information Act” (SB-1386), is a California state law that requires your organization to maintain personal information about individuals and inform them if the security of their information has been compromised.

> *“Don’t forget about all the other equipment connected to your network. Make sure everything is accounted for such as smart switches...”*

Raise Your Security Risk Awareness in Ten Steps

1

Policies

The creation of policies are an important part of the process of raising your company's security risk awareness. Management needs to approve and make the policies an official part of the rules and regulations of your company. Maintain policies on things such as: Internet access, electronic communication, remote access, BYOD, and privacy to make sure you're protected.

2

Provisioning servers

Maintain a checklist of everything that is running on each of the servers including IP address, location, patching, antivirus, remote access, and domain joined.

3

Deploying workstations

Computers are just as important as servers and are often our weakest points where viruses usually get propagated. Have a list of your workstations with naming conventions and user assigned to them. Make sure that they are running updated antivirus, the operating system software has the latest updates, that they comply with domain policies, they have working backup implementation, and all drives are encrypted.

4 Network equipment

Don’t forget about all the other equipment connected to your network. Make sure everything is accounted for such as smart switches that have the permissions allowing secure remote access, port restrictions to avoid users running promiscuous mode devices, and use secure routing protocols that use authentication.

5 Vulnerability scanning

Have your IT Service provider do weekly external scanning to compare control procedural changes.

6 Backups

Make sure your backups are being done and that you can confirm restoration regularly.

7 Remote access

Configure and maintain approved methods for remote access and grant permissions to only those users that should connect remotely, use two factor authentication, and set strong account lockout policies.

8 Wireless

Use SSID that cannot be easily associated with your company and use 802.1x authentication to your wireless. Create Bring Your Own Device policies or just prohibit users from bringing their personal equipment.

9 Email

Make sure you have an email filtering solution in place that can filter inbound and outbound email to not only protect your business but also your clients.

10 Internet Access

Provide users with secure Internet access by implementing an internet monitoring solution, filter lists, malware scanning, and port blocking.

With security risks on the rise, you need to protect your business. **Call us at Intivix and find out how we can help identify and address these and many other issues that represent potential risks for your business.** ■

GET IN TOUCH

605 Market Street, Suite 410
San Francisco, CA 94105

(415) 543 1033
intivix.com

GET IN TOUCH

605 Market Street, Suite 410
San Francisco, CA 94105

(415) 543 1033
intivix.com