VARAY
MANAGED IT

Cyber Security Assessment

Is your company vulnerable?

People	Answer #
How often do you provide security awareness training? 0 - We don't currently have security awareness training 1 - Once every 3+ years 2 - Once a year 3 - Monthly 4 - More than once a month	
Select all the topics that your Security Awareness Training covers: □ Password Management □ Social Engineering □ Identity Theft □ Malware □ Privacy/Pii □ Social Media □ Cloud Safety □ Data Security □ Mobile Security □ Working Remotely □ Online Safety □ Encryption	(.5 point per topic)
Is your training relevant to learner scenarios; are there hands-on opportunities to build security skills? 0 - We don't currently have training 1 - We provide generic training; it has hands-on activities 2 - We customize our training; it is primarily learning videos with some hands-on activities 3 - We customize our training; it always has hands-on Activities	
Does your company actively promote all types of training and continuous learning? 0 - No 1 - People try to fit in learning opportunities when possible 2 - We strongly encourage employees to take time for learning 3 - We fund all learning opportunities and staff actively receive time for learning	
If an unexpected email came from the CEO, what would your company culture allow? 0 - I have no idea 1 - People respond and do what is instructed 2 - Anyone can question an email sent from the CEO	
TOTAL (sum of answer #s)	

VARAY
MANAGED IT

Cyber Security Assessment

Is your company vulnerable?

Process	Answer #
What happens internally when someone leaves the company? Select the highest option that applies. 0 - We take them to happy hour 1 - We collect the laptop and badge 2 - We collect the laptop, badge and remove access to all applications except those, we have determined the employee needs after separation	
How does your organization view and address business and technology risk? 0 - Risk is an insurance matter 1 - Risk is the leadership team's job 2 - Risks are discussed across the company and plans developed 3 - Risk is mapped across all parts of the business with appropriate action plans in place	
Does your company have a cyber security or information security function (or team)? 0 - No 1 - We have an initial program that is somewhat documented but mostly individuals hold knowledge 2 - We have a documented program and actively work to mature it 3 - We have a defined security framework and regularly measure ourselves against it.	
When we create a new product or service, security is: 0 - The last thing we address 1 - Considered during development, but is a small part of our overall process 2 - Involved from the very first planning meeting through development, testing, and delivery	
Does your team discuss security between the various functions like finance and operations? Business and cyber security meet when there is an identified problem 0 - We talk about it when there is a problem. 1 - Security is a part of most or all initiatives. 2 - We integrate security objectives in all of our company planning and goal setting.	
TOTAL (sum of answer #s)	

VARAY
MANAGED IT

Cyber Security Assessment

Is your company vulnerable?

Technology	Answer #
How well do you keep an inventory of technology and information assets? 0 - Everyone buys whatever they want, and holds whatever information they need. 1 - The company buys and maintains basic technology and software, employees are free to use their own devices, no BYOD policy, no mobile device management (MDM) software, no management for information assets 2 - Company provides hardware (HW) and software (SW), BYOD policy, no MDM, no information asset management 3 - Company provided HW SW, BYOD Policy, MDM mandatory for sensitive information, no information asset management 4 - Company provided HW SW, BYOD policy, MDM mandatory for sensitive information, information assets are treated like physical assets	
Are systems kept up to date with patches and life cycled appropriately? 0 - Sometimes I might update something 1 - Patches are checked maybe once a year, systems are life cycled once they break 2 - Patches are checked once a quarter, we have some capacity planning and life cycle management 3 - Systems are set to automatically download and apply patches, systems are replaced or refreshed per recommended life cycle 4 - Patches are proactively managed by an IT service provider and checked periodically	
How regularly are logs reviewed and alerts monitored? 0 - What are logs? 1 - Some systems have local logging 2 - All systems are configured to log security related event information 3 - We have some centralized logging 4 - All critical systems are centrally logged, logs are reviewed on a regular basis	
Do you have an incident response plan? 0 - No 1 - Maybe - not sure where it is 2 - Yes, but not tested recently 3 - Yes, and tested recently	
Are critical systems and data backed up; when was the last time the backups were restored and tested? 0- No backups: never tested 1 - Maybe; but not sure to what extent 2 - Yes; but not tested recently 3 - Yes; and tested recently	
TOTAL (sum of answer #s)	

VARAY
MANAGED IT

Cyber Security Assessment

Is your company vulnerable?

Final Cyber Security Exercise Score	Total Score
People (Ideal Score Between 14-18 points)	
Process (Ideal Score Between 10-12 points))	
Technology (Ideal Score Between 14-18 points))	