

SECURITY: GET THE FACTS!

PROTECTION, DETECTION, RESPONSE Protecting your organization from the current threats to technology takes a three-pronged approach: protection, detection, and response.

- Protection: all things working to keep people out
- Detection: all things working to alert you when someone has gotten in
- Response: all things done to stop people from using your systems once they are in

DO YOU KNOW WHAT YOUR EMPLOYEES ARE DOING? Simple mistakes made by employees can have a devastating effect on your network's security. Actions such as opening an e-greeting card or downloading music may put your system at risk for potential exposure to outside sources. Make sure your employees are educated about what activities are considered "safe" and what activities should never occur.

DIGITAL ASSETS It is estimated that nearly 90% of all intellectual capital is in digital format ... and 50% of that is in an insecure e-mail at any given time.

YOU ARE RESPONSIBLE Companies are held accountable for any lost or stolen information, including confidential employee and customer information. By not protecting your company, you may stand to lose more than just a little information: you may lose valuable employees and essential customers.

WHAT'S IT ALL A-"BOT"? The term "bot" is one that is surfacing more and more in the technology field. And, you may not be familiar with what it really refers to. Generally, bots are software applications that run automated tasks over the Internet that are simple and repetitive. One of their largest uses is in an Internet search engine. But, they are increasingly used by criminals to illegally attack and gain control of a computer or computer system.

SPAM: EVERYONE'S ENEMY The use of spam is growing rapidly as hundreds of millions of e-mails are sent worldwide each day. In fact, so much spam is sent, sources seldom agree exactly what percentage of e-mail really is spam. Some report 40%, while others estimate the number closer to 95%. Either way, spam is a definite part of our e-mail lives – and a great potential threat to our computers and systems. Much of spam that is currently sent contains malicious codes meant to hack into the user's computer/network. A good rule of thumb: if you don't know the sender, don't open it. And, even if you do, read the subject line carefully to make sure it really is coming from a known source.



Working with **Integrity** is always the right decision.

1-888-764-8100

www.integrityts.com