Information Technology Security
for Small Business
(video script)

Descriptive Text for the Visually Impaired
August 11, 2009

By Joan Porter

Visual: Images related to computer and internet use and images symbolic of information technology security and cyber crime.

Narration:

"No matter how well you protect your business your information is still very much at risk and that puts your business at risk.

Visual: A computer keyboard and a cell phone.

Text: The words, "Names, Emails, Phone Numbers, Account Numbers, Files, Passwords, User Ids, Payroll, Internet Transactions, Credit Card Numbers, Electronic Commerce and Employee Databases" appear.

Narration:
"The dangers change and grow every day and the threats they pose to your business – and others – can be devastating."

Text: The words, "The best defense against these growing attacks?"appear.

Narration:

"The best defense against these growing attacks?"

Text: The words, "Information Technology Security for Small Business" and "It's not just good business. It's essential business" appear.

Narration:
"Information Technology Security. It's not just good business. It's essential business."

Visual: Scenes of employees working at computers and working in a variety of jobs at different kinds of small businesses.

Narration:

"Today protecting your business's information is just as critical as protecting every other asset you have – your property, your employees and your products. It doesn't matter what kind of business you're in or its size – whether you have one employee or 500. The fact is, your information is valuable and it's at risk."

Visual: Matthew Scholl, Group Manager, Security Management and Assurance Computer Security Division, NIST on camera.

"It's important that small businesses make IT security a top priority in order to protect their businesses. They make other security decisions everyday.
They lock their doors, they have alarm systems, they have trusted employees working behind the counters. They should exercise the same level of security and due diligence to their IT space where they have just as much exposure."

Visual: Richard Kissel, Information Security Analyst, Computer Security Division, NIST on camera.

"Cyberspace is a dangerous place to be. We all are there because we have to be there because that's where technology forces us to go right now. And if you don't understand that climate and the things that are involved there then you can get into trouble really quickly."

Visual: Jane Boorman, Project Manager, Office of Entrepreneurship Education, U.S. Small Business Administration on camera.

"There are some 26 million small businesses in this country and they all need to pay attention to the dangers of cyber crime. It's one of the greatest risks they face but many people don't realize it. Small businesses are "open for business!" They want their customers to come in but they're so open for business they sometimes don't take the time. They don't really realize that their entire business is at stake and when they are careless about their information technology protection, they can lose the entire business."

Visual: Matthew Scholl on camera

"The threats that are faced by small businesses are very similar to the threats faced by the federal government and large businesses as a whole. The truth of the matter is they don't care who you are. All they care about is that they can access your assets for their purposes."

Visual: An image showing the globe and a computer keyboard.

Text: The words, “Who are they?” appear.

Narration:

“But who are ‘they?’ Who is responsible for this?”

Text: The words, “Hackers; Experimenters and Vandals; Hacktivists; Cyber Criminals and Information Warriors” appear.

Narration:

“There are four main types of hackers. Experimenters and vandals are usually amateurs who do it for the thrill or to make a reputation for themselves. Hacktivists have a personal or political agenda. Cyber criminals are in it for the money. Other hackers are Information Warriors.”

Visual: Digital program code over image of Earth as seen from outer space.

Narration:

“They are professionals who work for nation-states which may have missions to disrupt the Internet for example, or take out a city’s electrical grid.”

Visual: Scenes of employees working at computers in a variety of kinds of businesses.

Narration:

“But all the dangers don’t come from the ‘outside.’ Businesses can be severely damaged - intentionally or unintentionally - by their own employees.”

Text: The words, “Insider Threats” appear.

Visual: Scenes of employees and computers at different businesses.

Narration:

“These ‘insider threats’ are responsible for nearly 80% of the problems that most small businesses have. No matter where the threat is coming from, the target is still the same −access to a business’s systems and information.”

Visual: Richard Kissel on camera

“The reality is that there’s dangers out there in all kinds of forms.”

Visual: Image of computer code – zeroes and ones.

Text: The words, “Theft of Data and Resources” appear.

Richard Kissel:
“You have theft of data, theft of resources, things like walking off with a laptop.”

Visual: Richard Kissell on camera

“You have the electronic PDAs of various kinds and literally some people run their businesses from these devices not understanding that all that sensitive information on those devices is vulnerable and it’s not encrypted, it’s not protected and so if they lose the device or somebody walks off with it all that data is gone. And may come back to haunt them later on.”

Visual: Image of a hacker typing on a laptop

Text: The words, “Denial-of-Service Attacks” appear.

Visual: Richard Kissel on camera

“You have other activities that nefarious folks can take and that’s denial-of-service where they just hammer a system until it just stops functioning and sometimes this is done to blackmail a business. They demonstrate that they can take down the system or the network and they say, ‘if you don’t pay us, we will take you out,’ and they mean it.”

Text: The words, “Malicious Code” appear.

Visual: Richard Kissel on camera

“Then you have people releasing malicious code. Once it gets on a system then it’ll do whatever it’s programmed to do. Malicious code can include things like keystroke loggers, which if somebody puts one on your system, it sits there and silently watches every keystroke you make which includes little things like bank account numbers, the passwords you use to get into your accounts, the answers you give to the security verification questions.”

Text: The word, “Viruses” appears.

Visual: Several computer screens

Richard Kissel:

“And viruses are a case of malicious code – and in terms of viruses there’s about 70,000 active viruses out there right now. The number goes up every year.”

Visual: Richard Kissel on camera

"So these are the kind of threats that we look at, we see out there. These are general classes of things that can go wrong and they all have the potential to damage or destroy an average small business."

Visual: Employees working at computers and a meeting of one company's employees.

Narration:

"A survey by the Computer Security Institute showed that a third of all data breaches in just one year came at the expense of businesses with 100 employees or less."

Text: The words, "Computer Security Institute Survey; 42% - Laptop Theft; 44% - Insider Abuse; 21% - Denial-of-Service Attacks; 50% - Computer Viruses" and "20% - Systems made into bots" appear.

Narration:

"Another survey of businesses – 23% of which were small businesses - showed that 42% reported laptop theft, 44% reported insider abuse, 21% reported denial-of- service attacks, 50% detected computer viruses and 20% reported systems being made into bots."

Visual: A variety of people in typing on computers and other activities at different types of businesses.

Narration:

"A bot is one of many computers that cybercriminals have taken over to make a botnet that they can use to attack other businesses, large industrial and even governmental systems. So, the vulnerability of one small business may not seem significant. But with over 26 million small businesses in the US, a threat that's common to a large percentage of them could pose a threat to the nation."

Visual: A variety of employees working at different businesses including offices, stores, restaurants and manufacturing.

Matt Scholl

"There are no silver bullets. So outsourcing is definitely an option that a small business can take to help them identify their risks and provide information security appropriately but it's important that a small business understand the basics of information security, what their risks are and the different ways they can mitigate those risks effectively. And that they should not solely rely on an outsourcing solution.

Information security can be an expense and there is a significant knowledge curve that needs to happen which is one of the reasons why we are doing this. Because in our belief this is essential to maintain the business and it can be done in a cost effective manner that is also effective for the small business owner.

We have an understanding of the small business as a part of the critical infrastructure of the nation economically and socially and its importance as a national asset that needs to be protected which is why SBA, FBI and NIST have partnered together on this work."

Visual: Employees working at a variety of businesses with logo representing NIST, SBA and the FBI's collaboration.

Text: The words, "Computer Security is Good Business" appear.

Narration:

"The collaboration between NIST, the Small Business Administration, and the FBI provides small businesses with a wealth of information and resources at the national and local levels including training and education, networking opportunities and practical assistance."

Visual: Scenes of people working and meeting at a variety of businesses.

Text: The words, "Right Investment; Define Needs; Security Practices; Stay Current" appear.

Narration:

"Business owners can learn how to make the right investment, define their information security needs, establish common security practices, and stay current. These are just a few of the topics available to help small businesses protect their information."

Visual: Image of a padlock on a computer motherboard and other images that represent information technology security.

Text: The words, "Information Technology Laboratory, Computer Security Resource Center" and web address "http://csrc.nist.gov/groups/SMA/sbc/index.html" appear.

Narration:

"The web site for NIST's Computer Security Resource Center can guide small business owners to the kind of help they need whether they're just getting started or staying up to date with the latest in information technology security."

Visual: Richard Kissel on camera

"There's a very small set of things, actions that a small business can do to avoid being an easy target. But they have to be done. And they have to be done consistently. So it's easy to avoid being the easy mark but you do have to work at it. You can't just sit still. You sit still and you're gone."

Text: The words, "Information Technology Security for Small Business" and "It's not just good business. It's essential business" appear.

Text: The following production credits appear.

Writer
Joan Porter

Videography
Chris Sciannella

Editors
Joanna Pearson
Chris Sciannella

Technical Advisor
Magdalena Benitez
Computer Security Division, NIST

Special Thanks To
Jane Boorman
U.S. Small Business Administration

Matthew Scholl
Computer Security Division, NIST

Richard Kissel
Computer Security Division, NIST

Executive Producer
Ron E. Meininger
NIST Public and Business Affairs

Disclaimer
The display of products and services in this program is for demonstration purposes only and does not imply an endorsement by NIST

Produced by
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce
July 2009

Visual: Fade to black