Stay a Step Ahead: Cybersecurity in Motion
Why updating cybersecurity is a necessity for small businesses

part one of three
No business too small, no threat too large

Small businesses may not realize it, but they are a big target for cybercriminals. As large corporations have invested millions in cybersecurity and elaborate training for their employees, the large number of small businesses who have yet to adapt to digital threats now present a far more tempting opportunity.

Fortunately, powerful new security measures have become more readily available to small businesses, and that technology has become more affordable. That’s good news for the 98.2 percent of American businesses with fewer than 100 employees, and the 89 percent – almost 1 million firms – with fewer than 20.

While these businesses often have limited funds available for technology and security, they also have more options available than before – many security enhancements have minimal cost and come mostly from training employees in common-sense procedures. New technology funding options, like equipment leases, or low-interest technology financing, put more tools at a business’ disposal.** And modern security software solutions offer exceptional value, protecting businesses better and more affordably than ever before.

up next...
Scaling cybersecurity for any size business

The only misconception more dangerous for small businesses than “I’m too small to do anything about it” is reality, as McAfee notes, not only are small businesses prime targets for hackers, but they are often more reliant on fewer devices – an entire business’ data may be hosted on a single laptop, or all its transactions conducted on a few mobile devices.

For these businesses, cybersecurity is absolutely mission-critical. One report found 47% of small businesses had at least one cyber attack in the past year.

Ransomware attacks were the most common, where data is locked and held for payment. But in addition to direct costs, there are also the harder-to-calculate costs of lost time, productivity and, if sensitive data was compromised, potential legal claims from clients.

The good news is that small businesses are not helpless. By closing off common avenues of attack, training employees (or themselves) to spot and repel attacks, and having up-to-date Antivirus subscription, such as McAfee Small Business Security, small business owners can reduce their risk and increase their security.

part two
Staying up-to-date in a changing landscape

With cybercriminals constantly adapting the techniques they use to target small businesses, it is critical that defenses be kept up to date. That means updating software, replacing software that is not supported, and upgrading hardware as new security features become available.

Learn how common software solutions, such as Microsoft Windows 7 and Microsoft Server 2008, are reaching their end of service life, what new security options are available in hardware, and how businesses can deploy them affordably.

Coming Tuesday, October 1st

part three
Equipping smart employees to use smart technology

Most cyberattacks are directly or indirectly enabled by (not noticed) by employees. Teaching people to practice good cybersecurity and equipping them with the right tools turns what can be the biggest vulnerability at a small business into its biggest security asset.

Learn about best practices in training and policies for small business security, and what tools they should use to make a business more robust and resilient in the face of threats.

Coming Wednesday, October 2nd
For small businesses to operate, it’s important not to take a “set it and forget it” approach. “Bigger companies are more likely on a fixed refresh cycle,” says Rohit Rao, a Senior Technology Advisor with Dell Technologies. “Small businesses tend to be less consistent. But it’s really important that they upgrade software, hardware and policies.”

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.

Despite being over a decade old, many small businesses still use these systems. After January 14, 2020, Microsoft will no longer release security updates or patches for the operating systems Windows Server 2008 or Windows 7.
Stay a Step Ahead: Cybersecurity in Motion

Why updating cybersecurity is a necessity for small businesses

part three of three

Equipping smart employees to use smart technology

Small business cyber security is a multi-layered dance that comes down to the right technology with people trained to use it, with upgrades and training on a regular schedule. But one size does not fit all.

Training employees is essential and can counter emerging threats. Still, many of the most serious cyberattacks facing small businesses actually use employees as a way in, and even require the employee to take some action to enable the attack.

"I tell my clients, security starts with behavior," said Rao. "The vast majority of threats start at the endpoints, somebody clicking on a link they shouldn’t be clicking on to a phishing email. Taking the time to train employees can go a long way to repelling the most successful types of cyberattacks."

Some good training to put in place to address top threats:

- Train employees to spot phishing. Often sent via email, phishing emails use email to direct people to legitimate-looking login pages to capture login credentials and then break into or infect systems. Teach employees to check the return email address and link. If anything seems off, don’t click the link, log in from a new browser window or call to ask about the email.
- Don’t click suspicious text links on phones. In a new tactic used to infect mobile devices, hackers text message a link to a target. Clicking it downloads and installs a hidden app that can capture information or provide a backdoor into a network.
- Establish a clear chain of approval for financial transactions. A simple scheme involves specifying an email to an employee, seemingly from a business leader, asking for an urgent financial transfer – right to the hacker’s account. Businesses should set up backup protocols to check the validity of transfer requests.
- Practice safe online habits: Set expectations about not visiting suspicious sites, not downloading unapproved software or media, and setting strong, unique passwords that are changed regularly.

Advice: Do as much as you can, and plan for the next phase.

"One of my customers was planning to buy 10 or 15 very, very basic computers," recalls Rao. "By understanding his needs, and working on the finances, we were able to get him better systems, plus a good firewall, and that’s had a huge impact on the overall security of his business."

The computers and devices employees use are different for business use as well, with added physical security features. Working with a consultant who can bundle solutions, offer financing** and establish what is truly necessary can help even the smallest businesses get strong security.

"Some products are tailored for home use, and some for business," said Bhoj Rao, a Senior Technology Advisor with Dell Small Business Solutions. "Small businesses, sometimes opt for home-use technology for budget reasons, but there is a difference when it comes to security."

Security starts with the overall network, says Rao. Small businesses are better served by a hardware firewall that’s designed to stop hackers from getting in, can analyze and prevent suspicious data before it gets to a computer, and can protect networked devices that don’t have software firewalls. For home use, a combined modem/router with less robust software-based firewall usually suffices.

<50% of small businesses train their employees in cybersecurity

(Better Business Bureau, 2017)

The computers and devices employees use are different for business use as well, with added physical security features. Working with a consultant who can bundle solutions, offer financing** and establish what is truly necessary can help even the smallest businesses get strong security.

"Some products are tailored for home use, and some for business," said Bhoj Rao, a Senior Technology Advisor with Dell Small Business Solutions. "Small businesses, sometimes opt for home-use technology for budget reasons, but there is a difference when it comes to security."

Security starts with the overall network, says Rao. Small businesses are better served by a hardware firewall that’s designed to stop hackers from getting in, can analyze and prevent suspicious data before it gets to a computer, and can protect networked devices that don’t have software firewalls. For home use, a combined modem/router with less robust software-based firewall usually suffices.

The computers and devices employees use are different for business use as well, with added physical security features. Working with a consultant who can bundle solutions, offer financing** and establish what is truly necessary can help even the smallest businesses get strong security.

"Some products are tailored for home use, and some for business," said Bhoj Rao, a Senior Technology Advisor with Dell Small Business Solutions. "Small businesses, sometimes opt for home-use technology for budget reasons, but there is a difference when it comes to security."

Security starts with the overall network, says Rao. Small businesses are better served by a hardware firewall that’s designed to stop hackers from getting in, can analyze and prevent suspicious data before it gets to a computer, and can protect networked devices that don’t have software firewalls. For home use, a combined modem/router with less robust software-based firewall usually suffices.

The computers and devices employees use are different for business use as well, with added physical security features. Working with a consultant who can bundle solutions, offer financing** and establish what is truly necessary can help even the smallest businesses get strong security.

"Some products are tailored for home use, and some for business," said Bhoj Rao, a Senior Technology Advisor with Dell Small Business Solutions. "Small businesses, sometimes opt for home-use technology for budget reasons, but there is a difference when it comes to security."

Security starts with the overall network, says Rao. Small businesses are better served by a hardware firewall that’s designed to stop hackers from getting in, can analyze and prevent suspicious data before it gets to a computer, and can protect networked devices that don’t have software firewalls. For home use, a combined modem/router with less robust software-based firewall usually suffices.

The computers and devices employees use are different for business use as well, with added physical security features. Working with a consultant who can bundle solutions, offer financing** and establish what is truly necessary can help even the smallest businesses get strong security.

"Some products are tailored for home use, and some for business," said Bhoj Rao, a Senior Technology Advisor with Dell Small Business Solutions. "Small businesses, sometimes opt for home-use technology for budget reasons, but there is a difference when it comes to security."

Security starts with the overall network, says Rao. Small businesses are better served by a hardware firewall that’s designed to stop hackers from getting in, can analyze and prevent suspicious data before it gets to a computer, and can protect networked devices that don’t have software firewalls. For home use, a combined modem/router with less robust software-based firewall usually suffices.