Defend, Detect and Repel
Part three of a three-part series on cybersecurity for small business

Fighting back: How small businesses can detect, respond and recover from a cyberattack

Even though 78% of cyberattacks are aimed at small businesses, only 15% of small businesses have a plan to deal with an attack.

This explains why small business cyberattacks can be so devastating. Losing money and data is just the tip of the iceberg. Loss of reputation, customers and intellectual property can compound the effects of an attack.

‘Attackers are getting very savvy,’ says Megan Wright, a Technology Advisor with Dell Small Business. They can be brutal as well. “The attacks are just more brutal as well. ‘The attacks are just more

Before an attack: Back up data and keep the network secure

Many cyberattacks are aimed squarely at your data. In ransomware attacks, data is held hostage for a cash payment. In other cases, hackers may be after information security like TPM 2.0 (Trusted Platform Module), fingerprint readers and facial recognition, and installing anti-virus and firewall solutions.

380 days: Average time threats remained undetected in networks
(Better Business Bureau, 2016)

Small businesses should assign someone to be responsible for information security. Often attackers go undetected because no one checked the firewall or anti-virus log, or ran needed updates.

Remember that networks evolve, and cracks can appear. Wright recalls one small business who said they’d been too busy to review how new hardware fit into the existing network. The resulting, preventable security gap allowed an attack that took the system down.

During an attack: Detect, report and react

The first rule is don’t panic. The second is to act fast. The employee tasked with security should immediately track down, isolate and remove the infection, or bring in someone who can.

But since many attacks come through email and the web, all employees should be trained to spot and report them. If they get a suspicious email, they should report it to leaders and IT immediately.

“I tell small businesses, security doesn’t just come from me as a technology advisor,” says Wright. “It has to be a priority for the entire business.”

Employees also need to be on the lookout for financial scams, like urgent orders to transfer money supposedly from business leaders. “Make it a policy to be over-cautious,” Wright says. “If it’s important, the sender will follow up.”

Defend, Detect and Repel
380 days: Average time threats remained undetected in networks
(Better Business Bureau, 2016)

Small businesses should assign someone to be responsible for information security. Often attackers go undetected because no one checked the firewall or anti-virus log, or ran needed updates.

Remember that networks evolve, and cracks can appear. Wright recalls one small business who said they’d been too busy to review how new hardware fit into the existing network. The resulting, preventable security gap allowed an attack that took the system down.

During an attack: Detect, report and react

The first rule is don’t panic. The second is to act fast. The employee tasked with security should immediately track down, isolate and remove the infection, or bring in someone who can.

But since many attacks come through email and the web, all employees should be trained to spot and report them. If they get a suspicious email, they should report it to leaders and IT immediately.

“I tell small businesses, security doesn’t just come from me as a technology advisor,” says Wright. “It has to be a priority for the entire business.”

Employees also need to be on the lookout for financial scams, like urgent orders to transfer money supposedly from business leaders. “Make it a policy to be over-cautious,” Wright says. “If it’s important, the sender will follow up.”

Defend, Detect and Repel
380 days: Average time threats remained undetected in networks
(Better Business Bureau, 2016)

Small businesses should assign someone to be responsible for information security. Often attackers go undetected because no one checked the firewall or anti-virus log, or ran needed updates.

Remember that networks evolve, and cracks can appear. Wright recalls one small business who said they’d been too busy to review how new hardware fit into the existing network. The resulting, preventable security gap allowed an attack that took the system down.

During an attack: Detect, report and react

The first rule is don’t panic. The second is to act fast. The employee tasked with security should immediately track down, isolate and remove the infection, or bring in someone who can.

But since many attacks come through email and the web, all employees should be trained to spot and report them. If they get a suspicious email, they should report it to leaders and IT immediately.

“I tell small businesses, security doesn’t just come from me as a technology advisor,” says Wright. “It has to be a priority for the entire business.”

Employees also need to be on the lookout for financial scams, like urgent orders to transfer money supposedly from business leaders. “Make it a policy to be over-cautious,” Wright says. “If it’s important, the sender will follow up.”

Defend, Detect and Repel
380 days: Average time threats remained undetected in networks
(Better Business Bureau, 2016)

Small businesses should assign someone to be responsible for information security. Often attackers go undetected because no one checked the firewall or anti-virus log, or ran needed updates.

Remember that networks evolve, and cracks can appear. Wright recalls one small business who said they’d been too busy to review how new hardware fit into the existing network. The resulting, preventable security gap allowed an attack that took the system down.

During an attack: Detect, report and react

The first rule is don’t panic. The second is to act fast. The employee tasked with security should immediately track down, isolate and remove the infection, or bring in someone who can.

But since many attacks come through email and the web, all employees should be trained to spot and report them. If they get a suspicious email, they should report it to leaders and IT immediately.

“I tell small businesses, security doesn’t just come from me as a technology advisor,” says Wright. “It has to be a priority for the entire business.”

Employees also need to be on the lookout for financial scams, like urgent orders to transfer money supposedly from business leaders. “Make it a policy to be over-cautious,” Wright says. “If it’s important, the sender will follow up.”

Defend, Detect and Repel
380 days: Average time threats remained undetected in networks
(Better Business Bureau, 2016)

Small businesses should assign someone to be responsible for information security. Often attackers go undetected because no one checked the firewall or anti-virus log, or ran needed updates.

Remember that networks evolve, and cracks can appear. Wright recalls one small business who said they’d been too busy to review how new hardware fit into the existing network. The resulting, preventable security gap allowed an attack that took the system down.

During an attack: Detect, report and react

The first rule is don’t panic. The second is to act fast. The employee tasked with security should immediately track down, isolate and remove the infection, or bring in someone who can.

But since many attacks come through email and the web, all employees should be trained to spot and report them. If they get a suspicious email, they should report it to leaders and IT immediately.

“I tell small businesses, security doesn’t just come from me as a technology advisor,” says Wright. “It has to be a priority for the entire business.”

Employees also need to be on the lookout for financial scams, like urgent orders to transfer money supposedly from business leaders. “Make it a policy to be over-cautious,” Wright says. “If it’s important, the sender will follow up.”