The Growing Importance of Cybersecurity & How Middle Market Companies Manage Cyber Risks
Cybersecurity is a growing concern

Since 2016, the percentage of middle market executives who are focused on cybersecurity issues jumped by 15 points. Leaders of upper middle market firms ($100M-$1B in annual revenue) and those operating in the financial, retail trade, and healthcare industries are the most likely to view cybersecurity as a highly important issue.

**OVERALL IMPORTANCE**

<table>
<thead>
<tr>
<th>2018</th>
<th>COMPARED TO 2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>71%</td>
<td>56%</td>
</tr>
</tbody>
</table>

**VIEW CYBERSECURITY AS EXTREMELY/VERY IMPORTANT**

**IMPORTANCE BY COMPANY REVENUE**

- **$10M-$50M**
  - 69%

- **$50M-$100M**
  - 63%

- **$100M-$1B**
  - 77%

**IMPORTANCE BY INDUSTRY**

**TOP THREE INDUSTRIES PLACING GREATEST IMPORTANCE ON CYBERSECURITY**

- **FINANCIAL SERVICES & INSURANCE**
- **RETAIL TRADE**
- **HEALTHCARE**
Reported attacks are slowly growing

Compared to two years ago, the percentage of middle market firms reporting cybersecurity attacks is up slightly. Estimates say, however, that breaches go undetected for about 200 days on average; many more companies have been attacked, therefore, than realize it at any given time. Phishing is the most commonly reported type of attack, followed by viruses or Trojan horses.

Companies that prioritize cybersecurity report higher growth

Middle market businesses that emphasize the critical nature of cybersecurity grow faster than their peers who view cybersecurity as less important. They experience somewhat higher revenue growth, and they add employees at a much faster rate than their counterparts.

**TOP SECURITY PRACTICES (TOTAL MM)**

**2018**

- 17% of companies say they have been a target of attack in the past 12 months

**COMPARSED TO 2016**

- 16% of companies say they have been a target of attack in the past 12 months

**OVERALL GROWTH**

- 9.8% revenue growth when cybersecurity is viewed as extremely important
- 8.9% revenue growth when cybersecurity is viewed as not very/at all important
- 7.9% employment growth when cybersecurity is viewed as extremely important
- 4.6% employment growth when cybersecurity is viewed as not very/at all important

**MOST COMMON TYPE OF ATTACK**

- 62% phishing
- 38% virus/trojan
The IT department typically leads cybersecurity efforts

In most middle market businesses, the IT department is responsible for cybersecurity. One out of 10 companies has its own cybersecurity department with a dedicated budget. Lower middle market companies are most likely to outsource cybersecurity, perhaps because they lack the resources or expertise to address it in-house. The lower middle market is also the most likely to leave responsibility for cybersecurity issues unassigned.
Cloud security and a well-trained staff are critical defenses

When building their defenses against attacks, the most common cybersecurity practice in place at middle market companies is training for the staff. Companies also invest in threat detection, risk management, and cloud security practices. Middle market leaders believe that a cloud security solution is the most critical piece of their defense strategy.
Vigilance is on the rise

Middle market businesses are more prepared for a cybersecurity attack now than they were two years ago. Nearly a third of companies currently align cyber risk management with broader strategic discussions; fewer than half of companies were doing the same in 2016. About four out of five companies have a documented plan in place to respond to threats or attacks. But aside from developing backup capabilities, fewer than half of middle market businesses have invested in other preventative measures.

### Overall Importance

<table>
<thead>
<tr>
<th>2018</th>
<th>Compared to 2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>62%</td>
<td>SAY CYBER RISK MANAGEMENT IS ACTIVELY PART OF BROADER STRATEGIC DISCUSSIONS</td>
</tr>
<tr>
<td>49%</td>
<td>SAY CYBER RISK MANAGEMENT IS ACTIVELY PART OF BROADER STRATEGIC DISCUSSIONS</td>
</tr>
</tbody>
</table>

### Incident Response Planning

<table>
<thead>
<tr>
<th>2018</th>
<th>Compared to 2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>79%</td>
<td>OF ORGANIZATIONS HAVE A DEFINED INCIDENT RESPONSE PLAN</td>
</tr>
<tr>
<td>73%</td>
<td>OF ORGANIZATIONS HAVE A DEFINED INCIDENT RESPONSE PLAN</td>
</tr>
<tr>
<td>36%</td>
<td>CYBER INSURANCE</td>
</tr>
</tbody>
</table>

### Preventive Methods

- **57%** BACK-UP CAPACITY
- **48%** SECURITY TOOLS & BEST PRACTICES
- **40%** HOSTING & SECURITY SOLUTIONS
Despite the rising importance of cybersecurity and increases in the steps companies are taking to protect themselves, middle market leaders have mixed feelings regarding the cybersecurity capabilities of staff and the effectiveness of their current solutions. Only half of the middle market leaders express high levels of confidence in their technical team, leadership oversight, and overall cybersecurity strategy.

**Confidence in knowledge and solutions is ambivalent**

**CONFIDENCE IN CYBERSECURITY SOLUTIONS**

- **52%** OF TOTAL MIDDLE MARKET EXTREMELY/VERY CONFIDENT

**CYBERSECURITY COMPETENCE RATING**

- **49%** RANK EXPERTISE OF THE TECHNICAL TEAM AS EXCELLENT/VERY GOOD
- **53%** RANK LEADERSHIP’S ABILITY TO GUIDE AND EVALUATE THE TECHNICAL TEAM AS EXCELLENT/VERY GOOD
- **14%** RANK EXPERTISE OF THE TECHNICAL TEAM AS FAIR/POOR
- **13%** RANK LEADERSHIP’S ABILITY TO GUIDE AND EVALUATE THE TECHNICAL TEAM AS FAIR/POOR

**About this report**

**WHO**

Self-administered online survey of 1,000 financial decision-makers at U.S. companies with annual revenues between $10 million and $1 billion.

**WHEN**

September 3, 2018 through September 14, 2018
From business as usual to business unusual, Fisher College of Business prepares students to go beyond and make an immediate impact in their careers through top-ranked programs, distinguished faculty and a vast network of partnerships that reaches from the surrounding business community to multinationals, nonprofits and startups across the globe. Our students are uniquely prepared and highly sought, leveraging Fisher’s rigorous, experiential learning environment with the resources of Ohio State, a premiere research university with 500,000 proud Buckeye alumni.

SunTrust Banks, Inc. (NYSE: STI) is a purpose-driven company dedicated to Lighting the Way to Financial Well-Being for the people, businesses, and communities it serves. Headquartered in Atlanta, the Company has two business segments: Consumer and Wholesale. Its flagship subsidiary, SunTrust Bank, operates an extensive branch and ATM network throughout the high-growth Southeast and Mid-Atlantic states, along with 24-hour digital access. Certain business lines serve consumer, commercial, corporate, and institutional clients nationally. As of December 31, 2017, SunTrust had total assets of $206 billion and total deposits of $161 billion. The Company provides deposit, credit, trust, investment, mortgage, asset management, securities brokerage, and capital market services. SunTrust leads onUp, a national movement inspiring Americans to build financial confidence. SunTrust’s Internet address is suntrust.com.

Founded in Chicago in 1924, Grant Thornton LLP (Grant Thornton) is the U.S. member firm of Grant Thornton International Ltd, one of the world’s leading organizations of independent audit, tax and advisory firms. Grant Thornton, which has revenues in excess of $1.7 billion and operates 59 offices, works with a broad range of dynamic publicly and privately held companies, government agencies, financial institutions, and civic and religious organizations.

“Grant Thornton” refers to Grant Thornton LLP, the U.S. member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. Services are delivered by the member firms. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another’s acts or omissions. Please see grantthornton.com for further details.

Cisco is the worldwide leader in IT that helps companies seize the opportunities of tomorrow by proving that amazing things can happen when you connect the previously unconnected. At Cisco customers come first and an integral part of our DNA is creating long-lasting customer partnerships and working with them to identify their needs and provide solutions that support their success. Learn more at cisco.com.