2017 Ransomware Poll
Global Results

July 2017
Number of Respondents =448

Respondents are global business and IT professionals who are members of ISACA.

Media Inquiries:
Kristen Kessinger, ISACA, +1.847.660.5512, *communications@isaca.org*

1. Do you think your company is prepared for a ransomware attack?

Highly Prepared	37%
Somewhat Prepared	**39%**
Not Sufficiently Prepared	17%
Not at all Prepared	5%
Unsure	3%

2. Has your organization experienced a ransomware attack?

Yes	27%
No	**63%**
Unsure	10%

3. If a ransomware attack were to hit your organization, do you think your organization would pay the ransom?

Yes	6%
No	**72%**
Unsure	23%

4. Did your company take any new precautions after the WannaCry attack?

Yes (please describe).	**50%**
No, and we don't need to	27%
No, but we should	13%
Unsure	10%

5. Will your organization take any new precautions in light of the Petya attack?

Yes (please describe).	28%
No, and we don't need to	**34%**
No, but we should	14%
Unsure	25%

6. Has your company conducted any ransomware training for staff?

Yes	**50%**
No	45%
Unsure	6%

7. How quickly does your organization apply the latest software patches?

Within 24 Hours of release	23%
Within one week of release	**29%**
Within one month of release	20%
Between one and three months of release	10%
More than three months after release	4%
We don't routinely patch our devices	4%
Unsure	10%

8. On a global scale, do you expect ransomware attacks will become more prevalent or less prevalent in the second half of 2017?

More prevalent	**83%**
Less prevalent	3%
Equally prevalent	11%
Unsure	3%

9. In what region do you live?

Africa	10%
Asia	**23%**
Europe	21%
Latin America	10%
Middle East	13%
North America	22%
Oceania	2%

10. How many employees does your organization have, including all locations?

Less than 50	10%
50-149	8%
150-499	13%
500-1499	17%
1500-4999	16%
5000-9999	7%
10000-14999	3%

More than 15000	**25%**

11. Which of the following, if any, best describes your business category?

Financial Banking	20%
Technology Services/Consulting	**24%**
Government/Military--National/State/Local	7%
Manufacturing/Engineering	5%
Healthcare	3%
Insurance	6%
Retail/Wholesale/Distribution	2%
Education/Student	4%
Telecommunications/Communications	4%
Public Accounting	3%
Transportation	2%
Mining/Construction/Petroleum/Agriculture	5%
Advertising/Marketing/Media	2%
Utilities	2%
Aerospace	0%
Legal/Law/Real Estate	2%
Pharmaceutical	2%
Other	8%

High Impact Quotes Attributable to Matt Loeb, CEO:

- "Surviving a cyberattack like Petya isn't just a question of response—it's a question of preparedness."
- "Our poll shows that more than one in four organizations typically wait longer than a month to apply the latest software patches. Given the escalating volume and complexity of threats enterprises are facing, placing greater urgency on rapid, comprehensive patching is a critical component of protecting an organization from the business- and infrastructure-crippling consequences of an attack."
- "WannaCry, Petya, Cryptolocker…ransomware will continue to be news and become the norm. What's needed is protection before an attack—not just a swift recovery afterwards."
- ***Every*** organization—either through training, frequent software updates, or hiring highly-skilled staff—needs to focus on being prepared for the next ransomware attack. Don't assume your enterprise 'might' be a victim of ransomware—assume it will."

Detailed Quotes Attributable to Tim Mason, SVP Operations and Chief Experience Officer:

- 'In a recent poll of our professional community, half of our respondents took action after WannaCry to add greater protection to their systems. These professionals don't see ransomware as an "if"—they see it as a "when," and they work to ensure their organization is prepared. That's a culture we've got to spread across the digital economy."
- We've polled our community, and there are some good signs—half of the companies said they have provided ransomware training to staff, and more than half of those organizations are applying software patches within the first few days they're available. That's great—for a start. Cyber security needs to be as common in the global economy as seatbelts are in cars. We've still got a long way to go until that happens."
- "While we've still got a substantial skills gap, we may be improving on creating a cyber security culture in organizations. After Petya, we asked participants within the global community about their organizations' preparedness for ransomware. Nearly 80% indicate some level of preparedness, with about 40% of those organizations telling us they're highly prepared."
- "The persistent launch of new attacks shows that traditional cyber security training is no longer adequate. The new norm must be situation-based training for unique scenarios as they surface. We've launched a cyber training platform giving Enterprises' always-on, always-updated lab training and assessment. Real-world training helps prepare for real-world readiness."