MARKET RESEARCH

Ransomware in the C-Suite: An (ISC)^2 Study

What Cybersecurity Leaders Need to Know About What Executives Need to Hear

(ISC)^2® | Inspiring a Safe and Secure Cyber World

INTRODUCTION

Ransomware was the biggest cybersecurity story of 2021. A spate of high-profile attacks causing widespread damage caught the attention of boardrooms across industries. Most of the conversation and analysis of these attacks focused on the damage done, attributing attacks to global cyber gangs and the debate about whether to pay ransoms. (ISC)^2 sought to learn how ransomware risk is viewed by executive teams, how confident they are in their defenses and what are their biggest concerns. Armed with this insight, cybersecurity professionals are better equipped to educate corporate leaders about ransomware and make a stronger case for investment in preventative measures and strategic response plans.

The study – which polled 750 U.S. and U.K. executives – provides cybersecurity professionals with a window into the thinking of the C-suite, as well as actionable insights into how they can more effectively communicate with executives about ransomware preparedness.

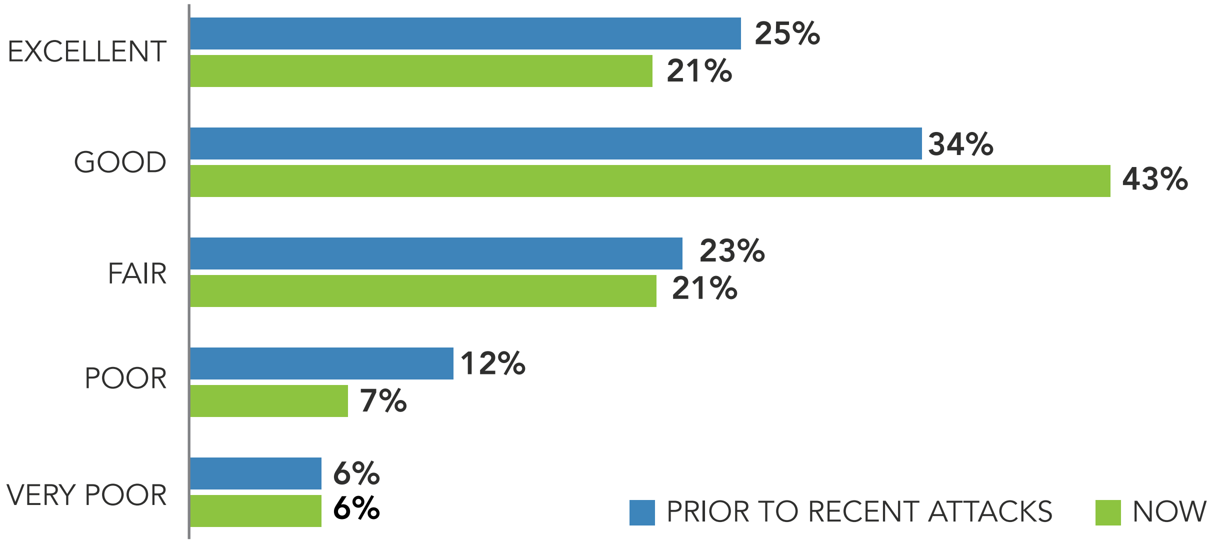
Awareness and Communications from Security Teams

(ISC)^2 polled executives with titles such as CEO, CFO, CIO, COO and General Counsel. Respondents were asked to rate their awareness of ransomware prior to high-profile 2021 breaches. 55% described themselves as very aware, and 40% said they were only somewhat aware. 59% of executives rated the communications they received from their cybersecurity teams about ransomware threats and mitigation tactics as excellent or good. Nearly one in five respondents (18%) rated those communications as either poor or very poor.

The executives were also asked how those communications have changed in the months following 2021's high-profile wave of ransomware attacks. While the percentage of those who indicated that the updates are excellent or good increased by 5%, that is still fewer than two-thirds of executives (64%) who highly rate those interactions.

THEN AND NOW

Rating Ransomware Communications from Cybersecurity Teams



Respondents were asked about the quality of communications they receive regarding ransomware before and after 2021's high-profile wave of ransomware attacks.

In terms of the frequency of those communications, 69% of respondents polled said the frequency of ransomware communications from their cybersecurity teams has increased since the recent attacks, while just 14% reported a decrease in communications.

What Do They Want to Know?

The attacks have spurred interest in cybersecurity security operations specific to ransomware, with the C-suite now asking cybersecurity professionals for more information on risks, defense strategies and budget needs.

When asked about the most critical information they need from the cybersecurity team, the biggest priority cited by 38% of respondents was for information on strategies to prevent ransomware from impacting data backup and restoration plans. Executives also want to know what it will take to restore minimal operations after compromise (33%), how prepared the organization is to engage law enforcement in the event of an attack (32%), and how prepared it is to engage cybersecurity investigators (30%).

TOP AREAS OF CONCERN FOR THE C-SUITE

Knowing how our security function is working with IT to ensure our back-ups and restoration plans will not also be impacted by any ransomware attacks	38%
Knowing what it will take to restore minimal operations if we were compromised (standing up back-ups, identifying priority systems, restoring basic services to meet basic mission needs)	33%
Knowing how prepared we are to engage with law enforcement	32%
Knowing how prepared we are to engage a cybersecurity firm to help investigate and respond	30%
Understanding where we are most vulnerable	30%
Knowing how we will operate if systems are compromised	30%
Understanding which third party systems we use or integrate with	30%
Understanding what our response plan is	29%

Cybersecurity professionals need to understand what the C-Suite wants to know about ransomare defenses and response plans. Cybersecurity teams should tailor communications accordingly to ensure their recommendations resonate with leadership.

TIP #1 for Cybersecurity Team Leaders: Increase Communication and Reporting to Leadership

The feedback is clear. Leadership wants and needs more communication from the cybersecurity practitioners dealing with ransomware within their organizations. There is also a need for more detail, depth and explanation in that reporting to ensure that leaders fully understand the landscape to facilitate more informed decisions and supporting calls for cybersecurity investment. Implement new reporting processes and create consensus with leadership about what information they care about most to deliver powerful reporting that supports the decision-making process.

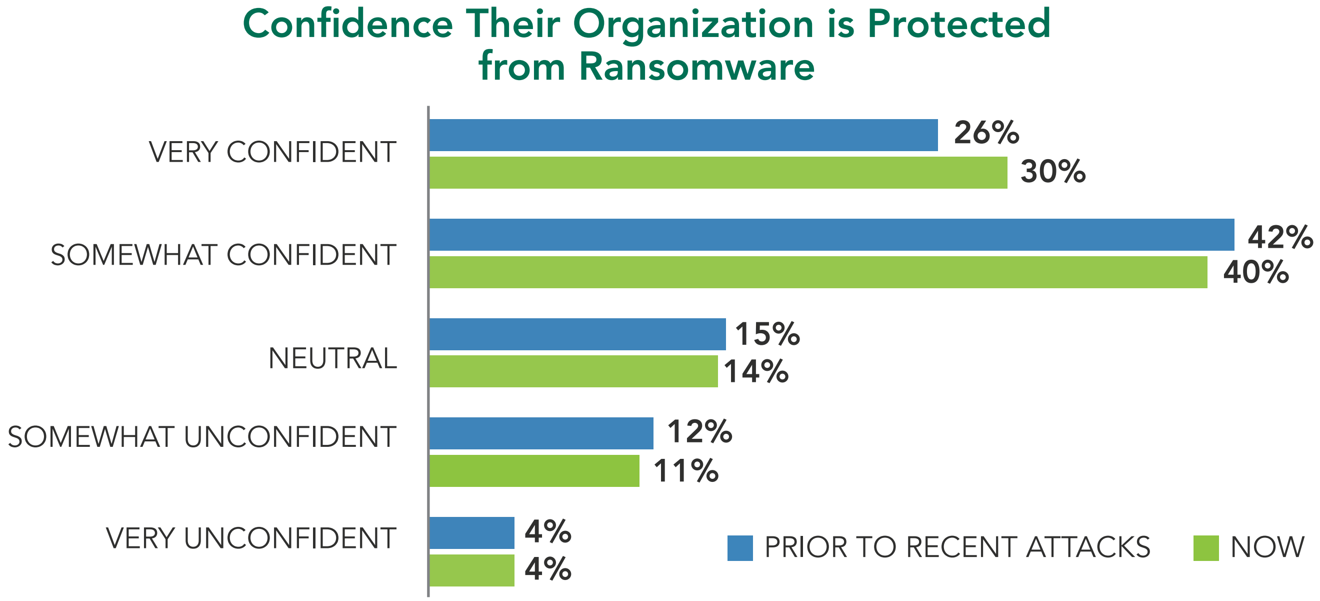
Asked what they would change about how cybersecurity teams communicate with them, executives underscored the need for budgetary and risk information. The C-suite wants more details on investments needed to protect against ransomware (43%), and how additional budget will improve the organization's security posture (40%). Budget questions are a higher priority for U.S. respondents than their U.K. counterparts, who place more importance on timely updates after major ransomware attacks occur to see if their organizations are "affected and/or protected."

Overall, 42% of respondents said they need more timely updates after major ransomware attacks to know if their organization was affected or if it is vulnerable. In addition, 38% of executives said they need clearer assessments of the risk to make informed decisions.

Too Confident?

Given the relatively low awareness they indicate about ransomware and the cited need for more detailed and frequent communications, respondents expressed high levels of confidence about their organizations' preparedness to handle a ransomware attack. The recent spate of attacks has not eroded that confidence either. In fact, there was a slight uptick in confidence (69% up to 71%) in the wake of the year's high-profile breaches. Only 15% of executives reported a lack of confidence.

ARE EXECUTIVES OVERCONFIDENT?



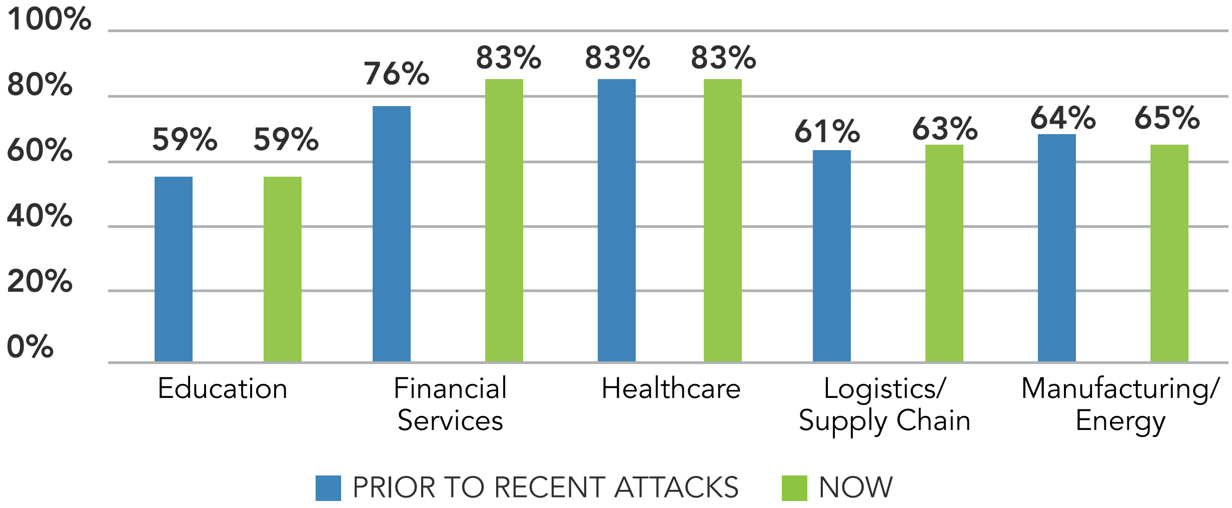
Cybersecurity professionals should consider how confident their leadership is in their organization's ability to defend against and respond to ransomware attacks. If there is a disconnect with reality, it's up to cybersecurity professionals to make that clear to their C-suite.

The uptick may seem counterintuitive, but it's possible that increased communications between executives and cybersecurity teams in 2021 has boosted overall confidence.

When it comes to ransomware preparedness, healthcare and finance executives reported the highest level of confidence (83% and 76%, respectively) prior to this year's ransomware events. Since the incidents. Since the incidents, confidence rose in financial services to 83% , while the often-targeted healthcare industry's confidence remained flat. Education executives reported the lowest confidence (59%) prior to the incidents, and it did not change in the aftermath.

CONFIDENCE ACROSS SECTORS

Confidence Their Organization is Prepared for Ransomware Attack (Very/Somewhat Confident by Sector)



We asked executives to rate how confident they felt about their organization being prepared for a ransomware attack. Only respondents in the financial services industry seemed to change their opinions in the wake of 2021's ransomware attacks.

TIP #2 for Cybersecurity Team Leaders: Temper Overconfidence as Needed

If cybersecurity professionals feel their C-suite is overconfident about ransomware, it's time to speak up and deliver a dose of reality. Be clear and realistic about the threats the organization faces and its ability to respond to a ransomware attack. Make the threat understandable and relatable. This isn't about dialing up the rhetoric, but being clear on the very real consequences ransomware can have on your operations and the long-term health of your organization.

What Worries Executives

If hit by a ransomware attack, the top concern among leaders, cited by 38% of respondents, is exposure to regulatory sanctions. The concern is higher in the United Kingdom (41%) than in the United States (36%).

The second biggest oncern (34%) for executives in the event of a ransomware attack is loss of data or intellectual property. This is followed by:

Loss of confidence among employees **31%**
Loss of business due to systems outage **31%**
Uncertainty that data wouldn't be compromised even after paying ransom **31%**
Reputational harm **31%**
Remediation costs **30%**
Loss of confidence in the organization's security **29%**

TIP #3 for Cybersecurity Team Leaders: Tailor Your Message

Depending on the kind of organization you work for and the types of data that the business manages, executive teams can have a variable level of risk tolerance. Understand and focus on the top areas of concern your executives care about most. For example, if regulatory compliance is a high priority, research which regulations you should be aware of and understand the implied consequences of non-compliance. Position risk to your leadership in a way that aligns specifically with their concerns, and build your reporting around what's most important.

DIFFERENT APPROACHES FOR DIFFERENT SETTINGS

Following the recent ransomware attacks, communications between the C-suite and cybersecurity professionals increased more in the U.K. (72%) than the U.S. (67%). The difference is statistically close but provides some insight on the differences in approaches to cybersecurity between the two countries.

Despite Brexit, the U.K. is still adhering to the European Union's General Data Protection Regulation (GDPR). The law requires organizations to report cyber breaches within 72 hours, while in the U.S. the timeliness of reporting breaches varies from one jurisdiction to another, with every one of the 50 states having a different breach notification law on the books. As of yet, there is no federal disclosure requirement, although the Cyber Incident Reporting Act of 2021 now awaits a vote in the U.S. Senate and would establish a 72-hour deadline for reporting any covered cyber incident against critical infrastructure, as well as a 24-hour deadline to report any ransom payments following a cyber incident.

Regarding the increased communications, there were also notable differences between industries. Healthcare, one of the most frequently targeted industries, reported the highest increase in communication frequency after the attacks, with 81% of respondents reporting an increase. Remarkably, in some industries – logistics, education, manufacturing and energy – communications have actually decreased.

Healthcare is also the industry that has had the most discussions regarding whether to pay ransom to attackers, with 89% of respondents saying they have talked about it, compared to 81% in finance, another industry often targeted. The lowest level of conversation on the subject has been in education (55%).

New Investments and Changes

Despite high confidence levels in current cybersecurity defenses, a solid majority of respondents (83%) said they are increasing their investments in ransomware defenses. Executives are willing to support improvements. Having seen the damage ransomware causes, including regulatory sanctions, executives may well now recognize the urgent need to protect their organizations.

In fact, only 14% of respondents indicated they are not putting any more money into ransomware defenses. For those who are, the biggest investments are in people. Hiring more security staff, cited by 33% of respondents, edged out other areas of investment, including:

Spending more on security technology **32%**
Spending more on outsourcing **31%**
Forming ransomware task forces **31%**

The focus on people demonstrates an understanding by the C-suite that technology alone cannot address all cybersecurity needs. Of course, recruiting cybersecurity professionals is a serious challenge in light of the 2.7 million worldwide skills shortage in the field. Nevertheless, cybersecurity professionals participating in the (ISC)^2 Cybersecurity Workforce Study 2021, advocate a people-first approach to closing the skills gap through a combination of retention and recruitment initiatives and a focus on "encouraging the development of future staff."

While considering ransomware risk, the C-suite is also preparing for how their organizations will respond in the event of an attack. Top priorities include cyber insurance with ransomware coverage (39%), establishing law enforcement contacts (37%) and creating Bitcoin accounts (35%). The rising popularity of cyber insurance is an indication of a risk-based approach to cybersecurity. The interest in Bitcoin accounts meanwhile, demonstrates a willingness to pay ransom if all else fails.

Study participants said their organizations have the following safeguards to protect against ransomware attacks, with some having at least two measures in place:

Cyber insurance with ransomware coverage 39%
Law enforcement contact(s) 37%
Ransomware task force/team 36%
Ransomware response plan 35%
Legal contact(s) 35%
Bitcoin account for ransomware payments 35%
Disaster recovery site 33%

TIP #4 for Cybersecurity Team Leaders: Make the Case for New Staff and Other Investments

Ensure you take advantage of a more receptive C-suite to not only make the case for technology investments but also push for more focus on building a resilient, deeper team of cybersecurity professionals.

To Pay or Not to Pay, That is the Question

Regarding whether to pay ransom, most executives (70%) said they have had discussions about it within their organization and 22% have not. The study revealed a majority of executive (64%) said they would consider paying if that proved to be the quickest way to restore operations. 31% said they would not pay, and 4% said they don't know.

U.K. respondents are more willing to pay (67%) than their counterparts in the U.S. (63%). By industry, healthcare executives are the most willing to pay (81%), compared to 64% in financial services, 59% in education and logistics, and 51% in manufacturing and energy.

Responsibility and Awareness

The (ISC)^2 ransomware study indicates a healthy level of awareness in the C-suite about the dangers of ransomware and its potential effects. But even though executives are taking some ownership of the problem by requesting more information from cybersecurity teams and investing more in defenses, most still see cybersecurity professionals as ultimately responsible for cyber defenses.

While 29% believe the ultimate responsibility for an organization's ransomware preparedness lies with the executive team, 70% attribute it to the cybersecurity or IT teams (35% each). Asked who is "most aware of the real-world risk of ransomware to the organization," 28% said it's the executive leadership team. 34% believe the leadership and cybersecurity teams are equally aware of cyber risks, while another 34% said the cybersecurity team has the most awareness.

TIP #5 for Cybersecurity Team Leaders: Make Clear that Ransomware Defense is Everyone's Responsibility

Our study showed that responsibility is not clear cut in the minds of the C-suite, with an even spread of ownership between cybersecurity, IT and executive leadership. It is important that organizations embrace the fact that ransomware defense is everyone's responsibility and avoid compartmentalizing responsibility and visibility of ransomware knowledge, policies and processes. Only 28% of respondents stated that ultimate responsibility rests with the executive team. Ultimately, leadership must come from the top of the organization in all instances, but it is the responsibility of cybersecuity professionals to inform and educate senior leadership about the growing ransomware threat.

CONCLUSION

The findings show that while C-suite executives want more detailed and frequent updates from their cybersecurity teams on ransomware, by and large they are also willing to invest more in defenses and people.

For cybersecurity leaders, the study's findings indicate now is an opportune time to talk to the executive team about which investments organizations should be making in people, technology and processes. With ransomware now prominently on the minds of executives, the timing is ideal to ask for the support cybersecurity teams need to protect their organizations against ransomware.

Cybersecurity professionals should keep the following golden rules in mind when communicating with the C-suite about ransomware.

1. **Communicate More Frequently with Leadership**
2. **Temper Overconfidence As Needed**
3. **Tailor Your Message to What Concerns Leadership the Most**
4. **Make a Strong Case for More Security Staff**
5. **Make Ransomware Defense Everyone's Responsibility**

Methodology

The (ISC)^2 Ransomware Study was a blind survey conducted by (ISC)^2 and Opinion Matters in September 2021. The total respondent base included 750 C-suite executives (CEO, CFO, CIO, COO, General Counsel/CLO, President) from organizations with more than 500 employees. 500 respondents were from the U.S. and 250 from the U.K. The margin of error is plus or minus 3.6% at 95% confidence level.

About (ISC)^2

(ISC)^2 is an international nonprofit membership association focused on inspiring a safe and secure cyber world. Best known for the acclaimed Certified Information Systems Security Professional (CISSP®) certification, (ISC)^2 offers a portfolio of credentials that are part of a holistic, pragmatic approach to security. Our membership, more than 160,000 strong, is made up of certified cyber, information, software and infrastructure security professionals who are making a difference and helping to advance the industry. Our vision is supported by our commitment to educate and reach the general public through our charitable foundation – The Center for Cyber Safety and Education™. For more information on (ISC)^2, visit www.isc2.org, follow us on Twitter or connect with us on Facebook and LinkedIn.

© 2021, (ISC)^2 Inc., (ISC)^2, CISSP, SSCP, CCSP, CAP, CSSLP, HCISPP, and CBK are registered marks of (ISC)^2, Inc.

CISSP. ISSAP. ISSEP. ISSMP. SSCP. CCSP. CAP. CSSLP. HCISPP.