UMass | Dartmouth

CHARLTON COLLEGE OF BUSINESS

University of Massachusetts Dartmouth's
2nd Annual Employee Threat Readiness Survey ©
Significant Employee Cyber Vulnerabilities Continue

By Drs. Timothy Shea and Steven White

July 2018

Introduction

In 2018 it is common knowledge that cyber security is a large and growing problem. What we sometimes forget among the many reports of cyber intrusions is that at least 50% of the cyber security problem is due to us, the everyday user, not protecting ourselves and our companies -- for example, poor passwords, responding to an email phishing attack, or being careless about protecting our laptop when we travel.

The University of Massachusetts Dartmouth's Charlton College of Business recently completed their 2nd Annual Employee Threat Readiness Survey. The goal of the survey is to see how well companies are managing the risk their employees bring to cyber-security by asking employees about their awareness and training in regards to cyber-safety and their competence in safely handling daily cyber-security risks. In conjunction with Qualtrics market research, the data set has almost 800 usable respondents, from across the United States, balanced by gender, age, income, ethnicity, education, and location. The results presented below will include results from both the 1st survey in the fall of 2016 (done in conjunction with AYTM market research) and the 2nd survey in the spring of 2018.

"Knowing"

Employee cyber-safety, the "human firewall", develops first from employees becoming aware of the problem – that is, "knowing" there is a problem and that it is important. This is the first part of the three-part equation. Companies help the process through a variety of communications and policies to help create awareness. Two questions were asked:

	Strongly Agree or Agree	
	Year 1	Year 2
Your employer has ensured that you have read the company's cyber security policies and has made it clear what is expected of you.	73%	68%
Your company's senior leadership communicates with everyone about expectations for cyber safety practices.	69%	73%
Average	71%	69%

The scores are pretty good and pretty consistent across the 2 years of data -- an average of 70% of the employees agree their company does well in terms of making company cyber security policies known along with senior leadership expectations. However, that does leave 30% who do not agree. That number is far too high. A true culture of cyber-safety, a "human firewall", requires close to 100% engagement. There is still work to do. In the current survey, an additional question was asked to assess whether the most basic message – cyber security is important – had been conveyed by the company:

Your employer considers cyber security to be important	75%

Again, while 75% represents 3 out of 4 employees, work is still needed to get that message across to all employees. Part of the solution is repeated messaging. For example, how often is the company getting its message out? From the survey results only about 2 out of 3 companies communicate about cyber security at least every quarter (Year 1 = 64%, Year 2 = 71%).

The next section looks at the second part of the three-part equation – "Doing, Part 1". This section looks at the kind of training being offered in companies to help mitigate employee risk.

"Doing", Part 1

The second part of the three-part equation is how well employees are prepared for specific responses to cyber-threats – that is, "doing". Training is a big component in this effort. Employees were asked if they had training to handle common day-to-day cyber-security challenges. The results follow:

For which of the following activities does your company provide cyber safety communications?

	Year 1	Year 2
Providing strong requirements on password composition and regular password changing	64%	51%
Understanding what is considered Personal Identifiable Information and how to keep it confidential	55%	43%
Protecting sensitive information when traveling or working remotely	49%	40%
Connecting personal devices to the company network	46%	36%
Detecting and handling emails that you suspect are false or phishing	63%	58%
Giving out sensitive information over the phone	46%	39%
Recognizing warning signs if other workers' behavior seems suspicious	40%	29%
Leaving your computer where sensitive information could be seen or	54%	37%

the computer could be stolen		
Using external machines or USB sticks at work	40%	27%
Average	51%	40%

Surprisingly, there was a drop in training, across the board, from 51% overall to 40%. However, the rank order was consistent, with the 3 topics with the most training the same in both years – passwords, emails and what is considered personal identifiable information. Likewise, the least reported training was for the same 2 topics – recognizing warning signs in others and using USB sticks at work. There was less training reported in the more recent survey but each year showed similar rankings in what training was most and least important.

Regardless of which year of data, the results are eye-opening. These important cyber-security topics needed for working safely day-to-day are not being covered, on average, for over half of the employees in companies. It may speak to motivation by companies or perhaps the lack of an effective training program that impacts behavior across a company.

The nature of the training also need improvement. While the results show training is trending towards more effective shorter modules, less than 2 out of 3 employees found the training engaging and memorable.

	Year 1	Year 2
The percent of company training and communications that are 14 minutes or less.	41%	46%
	Strongly Agree or Agree	
The modules were considered engaging and memorable.	65%	51%

In the 2nd year, two additional questions were asked to measure whether the training was effective and provided value. Sixty-five percent agreed. Again, more than one-third of the employees disagreed.

Finally, a similar percentage of employees – two-thirds -- are comfortable they have a prescribed process for reporting suspected security breaches as well as access to support, when needed.

	Year 1	Year 2
Your company provides easy access to support and guidance to cyber-safety questions when they arise.	70%	66%
Your Company has a clearly defined process for reporting actual or suspected security breaches.	70%	68%

In summary, there appear to be challenges for companies in providing comprehensive communications and training. Two out of three employees trained is not enough. The next section looks at self-reported employee competence in handling cyber security challenges from the employee's perspective.

New Information: Self-reported Competence – "Doing", Part II

New information collected in the 2nd year of the survey included self-reported competence by the employees in handling the day-to-day challenges of being cyber-safe – that is, being an effective member of the "human firewall". This is the third part of the equation – competence. It is not enough to just be aware and take training. How much did you learn? How has your behavior changed when confronted with cyber-security issues? Overall, employees feel more confident than the level of training might suggest:

	Year 2
I can recognize emails that should not be opened because they may be dangerous	79%
I can recognize emails that might be fake and ask for log-in information	79%
I can recognize emails that may contain malicious links or downloads	79%
I have a process in place to protect my passwords from being stolen	71%
I know how to protect information when traveling or working remotely	71%
I know what steps I should take should I suspect a cyber-security issue or problem	75%
I know how to validate requests for information	72%
I feel empowered to say no to a request for information even if later it turns out to be from a legitimate source	73%
Average	75%

The self-reported competence questions' results seem encouraging. Three-quarters of employees consider themselves prepared to handle a number of standard, day-to-day, cyber-security challenges. However, when asked about "others" in the company and their training and competence, the results drop significantly, to about 60 percent.

	Year 2
You feel that your co-workers are prepared to recognize cyber-attacks	59%
You feel that your co-workers are prepared to avoid cyber-attacks	60%

Both sets of numbers re-enforce that more work is needed to create a comprehensive and competent culture of cyber safety.

Conclusion

The stakes are too high. Risky cyber behavior at work can cause significant damage to a company. The results from two years of data show that current efforts are only impacting about two-thirds of the employees. With a problem like cyber-security, full participation is essential – the "human firewall" is only as good as its weakest link. There is a high level of risk that still needs to be addressed in today's workforce.

So, what is next? How do we win the cyber-security war on the human front? How do we strengthen the "human firewall"? One way is to assess a company's "human firewall" for its risk level. A second is to upgrade training and communications levels:

1. First, at the organization level, the survey and results will soon be refined into an audit tool that companies will be able to use in order to assess cyber-risk among employees.
2. Secondly, in order to impact behavior across the workforce, companies may need to employ a more sophisticated and comprehensive means of cyber-security training. ThreatReady Resources is one company expert in more advanced cyber-security training techniques – affordable, longer term training that is engaging and impactful. In other words, training that helps change behavior and ingrain a deep corporate culture.