Security Awareness Training

How to Create a Culture of Security Awareness

The rapid spread of ransomware thanks to email phishing shows again that security is only as effective as the humans entrusted with it. Find out from our 2016/2017 Security and Risk Management Benchmark and Maturity Model how to make every member of your organization security aware.

Compass Direction Points:

- **Regulators are mandating cybersecurity training.** The NYS DFS “Part 500 Regulations” now in effect—understand the requirement, it may apply to you before long! Page 5
- **Budgets and priorities don’t always align.** Security teams rate training among top-3 priorities—IT needs to make sure budgets reflect this. Page 8
- **People more likely to remember an enjoyable training video.** Communicate with people the way they need you to. Page 11

By Johna Till Johnson
CEO
Nemertes Research
# Table of Contents

COMPASS DIRECTION POINTS: .......................................................... 1

TABLE OF FIGURES ........................................................................ 4

EXECUTIVE SUMMARY ................................................................. 5

THE ISSUE: NETWORK SECURITY CAN’T SAVE USERS FROM THEMSELVES 6

THE STATE OF SECURITY AWARENESS TRAINING .......................... 6

The Importance of Security Awareness Training .............................. 6
Security Can Spend on Training ..................................................... 8
Security Not Ramping Up Spending In Line With Importance of Training 8
Not Just About Budgets ................................................................. 9

BUILDING AN AWARENESS CULTURE ...................................... 9

Awareness ..................................................................................... 10
Training ......................................................................................... 10
Professional Development (Organizations and Certifications) ......... 10

DEVELOPING A SECURITY AWARENESS TRAINING PROGRAM .......... 10

Phase 1: Assessment ................................................................. 10
Typical security challenges ......................................................... 11
Phase 2: Planning ................................................................. 11
Phase 3: Development .......................................................... 12
Short animated videos ............................................................... 13
Online interactive quiz .............................................................. 13
Printable checklist ..................................................................... 13
Online, web-based, and in-person education and communication ... 13
Dry runs ......................................................................................... 13
Phase 4: Implementation ......................................................... 14
Phase 5: Ongoing Support ....................................................... 14
Third-Party Awareness Training Vendors ................................. 14

CONCLUSION AND RECOMMENDATIONS ............................... 15

APPENDIX A: NEMERTES SECURITY MATURITY MODEL ............. 16

Level 0: Unprepared .................................................................... 16
Level 1: Reactive .......................................................................... 17
Level 2: Proactive ......................................................................... 17
Level 3: Anticipatory .................................................................... 17
Maturity Model Elements ........................................................ 18
Bellwether Technologies: Definition ......................................... 18
| COMPANY SIZE: REVENUE | 21 |
| COMPANY SIZE: EMPLOYEES | 22 |
| PARTICIPANTS: BY INDUSTRY | 23 |
| PARTICIPANTS: BY TITLE | 24 |
| PARTICIPANTS: BY IT CULTURE | 25 |
Table of Figures

FIGURE 1: TOP SECURITY CHALLENGES .......................................................... 7
FIGURE 2: BUDGET BREAKDOWN .............................................................. 8
FIGURE 3: SECURITY SPENDING INCREASES .............................................. 9
FIGURE 4: THE NEMERTES MATURITY MODEL ........................................... 16
FIGURE 5: BUSINESS IMPACT OF INFORMATION SECURITY MATURITY ........ 17
FIGURE 6: ELEMENTS OF THE MATURITY MODEL ..................................... 18
FIGURE 7: PARTICIPANTS’ COMPANY SIZE BY REVENUE ............................ 22
FIGURE 8: PARTICIPANTS’ COMPANY SIZE BY EMPLOYEES ......................... 23
FIGURE 9: PARTICIPANTS BY INDUSTRY ................................................ 24
FIGURE 10: PARTICIPANT JOB TITLES ..................................................... 25
FIGURE 11: PARTICIPANTS BY IT CULTURE .......................................... 26
Executive Summary

The recent success of Ransomware as a Service (RaaS) attacks has thousands of companies facing systematized extortion. The enterprise facing the decision of whether “to pay or not to pay” can usually thank an unaware employee—even a CEO—who fell victim to the oldest cybersecurity ruse, the phishing email.

The best defense against cybersecurity threats is a security-aware culture that permeates the entire organization and which touches anyone on the network—from the board to the lowest intern. For this culture to reach beyond the IT security team, enterprises must implement targeted and sustained security awareness training.

Best-of-the-best security organizations consistently rate security awareness training as a top challenge. Yet when it comes to budgeting, companies often give training short shrift. The training budget and other factors will influence how a company approaches training.

Whether a company develops an in-house security awareness training program or opts to outsource to a third party, the steps must remain the same: assess, plan, develop, implement, monitor and maintain.

• **Assess** the company’s training needs: This involves interviewing employees and leaders to rate their knowledge of security issues and best practices, as well as their willingness to learn and their learning styles, via interviews, questionnaires, and even personality tests like Myers–Briggs.

• **Plan:** Make a list of training topics, prioritized to most-urgent training needs. Decide whether to train in-house or to hire a third-party training vendor.

• **Develop** a set of custom modules, each module addressing a specific training need and goal, and testing and metrics to go along with each module.

• **Implement**: roll out the training program modules, testing, and metrics.

• **Monitor and maintain**: gather regular feedback to determine the program’s effectiveness and to drive updates to it. Effective feedback methods include surveys, short online refresher videos, and community engagement.

If a company lacks the time or manpower needed to implement the above steps, increasingly many third-party companies specialize in customizable training.
The Issue: Network Security Can’t Save Users From Themselves

The most disturbing cybersecurity trend of 2016 has been the “Ransomware as a Service” (RaaS) phenomenon. Security Awareness Training is crucial to building a bulwark against RaaS, along with endpoint security and endpoint backup.

Most ransomware arrives via standard phishing attacks in the form of downloaded executables or links clicked. Nemucod, for instance, arrives as an email ZIP attachment pretending to be an invoice and containing an infected executable JavaScript file. Employees should know better than to click on invoices from parties they don’t recognize, but thousands do, every day. The truth is that phishing is here to stay. “Phishing attacks, spearphishing, whaling—it’s the attack vector of choice for sophisticated cybercriminals, because it works,” says the CSO at a large financial services company.

Security awareness training will not completely solve the problems of ransomware or spearfishing, but it will greatly reduce them. But reducing email threats isn’t the only goal of training. An effective training program should create resistance to social engineering. Other important training goals include improving overall workplace security (e.g. things like locking screens when leaving the desk, and not sharing passwords) and introducing general best practices, like creating strong passwords (and not writing them on post-it notes).

Nemertes envisions the security awareness training initiative as a multi-faceted, multimedia outreach, with associated metrics.

The State of Security Awareness Training

If training is a critical layer in any defense-in-depth strategy, it is important that IT recognize it as such; that it have the ability to put money into training (i.e. that it not be wholly under the control of some other department); and that it invest. For a training program to succeed as part of a larger cultural change, leadership buy-in is critical. “We have business unit presidents doing video blogs on why security is important,” says one CSO at a very large professional services company.

The Importance of Security Awareness Training

We asked participants in Nemertes 2016-17 Cybersecurity and Risk Management research an open-ended question about their top security challenges, and found their responses fit into a handful of categories. (Please see Figure 1.) The top three categories were:

“Phishing attacks, spearphishing, whaling—it’s the attack vector of choice because it works.”

– CSO at very large financial services company
1. Security Fundamentals (41.2%). This is a catch-all term for implementing basic security functions and processes (anti-malware, firewalls, patches).

2. Employee Awareness and Insider Threat (29.4%) This covers all aspects of training users and protecting the environment against inside attacks, both witting and unwitting.

3. Compliance, regulations, and risk management (29.4%). This covers the business, legal, and regulatory risks associated with security.

In explaining the importance of training and other measures in mitigating the insider threat, the CISO of a large educational institution put it this way: “My top security challenge is stupid people, and my motto is ‘you can’t stop stupid but you can slow it down’. My job is slowing down stupid.”

![Figure 1: Top Security Challenges](image)

The impetus to train staff is now getting a boost in importance from that third top challenge: regulatory compliance. States are beginning to pass laws which mandate cybersecurity training, such as the New York State Department of Financial Services’ (NYS DFS) “Part 500” regulations, which went into effect in January 2017.
Nemertes believes that the ramifications of these regulations will be felt far beyond New York–based financial services firms: All states, and most industries, will eventually adopt requirements similar to these. Therefore, while these regulations are obviously of greatest urgency for NYS-based financial services firms, enterprise cybersecurity professionals at all types of companies, and cybersecurity vendors and service providers should pay close attention. Nemertes believes this regulation will be a model for other states and the federal government.

**Security Can Spend on Training**

Fully 100% of benchmark participants said they budgeted for education, awareness, and training. (Please see Figure 2.)

![Security Budget Breakdown](image)

**Security Not Ramping Up Spending In Line With Importance of Training**

Most security budgets are rising. However, Nemertes found a clear mismatch between the areas of increase and the afore-mentioned areas of “top concern.” Even though participants rank “training, education and awareness” as their number two “top challenge,” it ranks merely fifth as a spending priority. (Please see Figure 3.)
The technologies like multifactor authentication and initiatives like automation that security leaders rely on to address challenges like phishing are similarly far down the stack.

In short, there's a misalignment between the areas that benchmark participants say matter to them, and where they're actually investing.

**Not Just About Budgets**
Just as the size and revenue of a company will influence the training budget, human capital factors such as time, expertise and priorities will also influence how a company approaches training. Staff can choose to create their own security awareness training program or to hire a third-party vendor, or develop a hybrid approach utilizing both. Many specialist companies can help develop training programs. It is imperative that security teams customize training according to a company's needs, and avoid the temptation to rely solely on off-the-shelf solutions.

**Building an Awareness Culture**
IT teams are the keepers of a security-aware culture. Aspects of this culture include awareness, training, and professional development. The key to changing a company’s security awareness culture is evangelization—spreading the security team's culture outward to every member of the organization.
Awareness

Every member of the organization has to focus some attention on security. “We’re interacting more and more with the business people,” says one CISO of a large financial services company. “We’re in front of a board presenting several times a month. We have really strong security awareness. We had someone from my team in front of every single employee to provide security training on what they need to do to protect the firm.”

Training

Building staff awareness requires producing and/or providing relevant security skills and competency training. The security team is typically the focus of formal training, either internally or externally. But well-trained security staff should leverage their training to train others in turn on how to implement best practices throughout the organization.

Professional Development (Organizations and Certifications)

Professional development implies a guarantee that IT personnel meet standards because they have been evaluated against measurable criteria. Focused professional development should be extended to every employee who is connected to the company’s network or who interacts with its data systems.

A successful practice among the U.S. military services is the “Train the Trainer” model. All employees with significant security responsibilities and who receive specialized training can become trainers themselves. Security teams should routinely consider which aspects of their formal training can be streamlined to meet the training needs of the entire group.

Developing a Security Awareness Training Program

Whether companies stand up their own internal training programs, or decide to go with a trusted third-party vendor, the steps to creating a custom training program are the same: Assess, Plan, Develop, Implement, Follow up.

Phase 1: Assessment

For each security topic, IT needs to deliver a multimedia content “module,” described in greater depth below. To select appropriate modules, InfoSec teams must uncover the areas of greatest need, and agree upon appropriate metrics to measure improvement in security awareness and behavior.

The first step is to interview security principals to uncover:

- A prioritized set of security issues
- Examples of existing challenges
• Appropriate metrics for improvement

Additionally, course developers need to assess the security needs and awareness levels of all non-IT staff.

Typical security challenges
Although there’s always something new to cover, mostly even the new material will fall into one of these perennially important categories:

• Email security: Best practices for avoiding phishing and other email attacks
• APT awareness: Insight into advanced persistent threats (APTs), how they’re structured, and how they can be protected against
• Password and authentication best practices: What not to do when setting passwords and granting access to critical resources
• Content and intellectual property protection: Key steps for ensuring intellectual property remains protected
• User device protection. As companies have migrated to BYOD models for smartphones and, increasingly, tablets and other devices, they’ve opened new avenues for attackers. Users increasingly bear the brunt of protecting their own devices, and need to understand the ins and outs of device protection.
• Minimizing the cloud footprint. It’s surprising how much information can be collected from public-cloud usage patterns. For individual consumers, the degree to which this is a concern is their own business. But when this information can be used by hackers as part of APTs, employees must learn to minimize their work-related footprints.
• Staying alert to social engineering. It’s a sad fact that after a quarter-century of cybersecurity, the simplest approaches remain the most effective. Users are all too eager to give away their passwords, attach unknown thumb drives to machines, and leave personal information on post-it notes. The emergence of embedded video cameras just adds another layer of vulnerability—now intrepid hackers can watch users go about their daily tasks.

These are examples of typical challenges facing employees at most organizations, but each organization will likely have unique challenges.

Phase 2: Planning
Once an InfoSec team has identified and agreed upon a definitive set of issues, the next phase begins, planning the necessary set of training modules, their sequence and relationships, and the means by which IT or HR can assess user understanding before and after training.
This phase includes writing a Training Management Plan (TMP), identifying trainers, and considering the logistics necessary to implement the plan.

The TMP—sometimes called a Course Management Plan (CMP), or Learning Management Plan (LMP)—is a set of detailed yet clear instructions stipulating how managers and instructors (and anyone else involved) will carry out training and evaluation.

The TMP is the go-to reference for the training program. It contains schedules, catalogues all course materials, and lists pre-implementation tasks including:

- Scheduling and notifying trainers and trainees
- Ensuring all course materials such as lesson outlines and learning activities are ready
- Allocating classroom space
- Procuring all necessary equipment and supplies

Including a training calendar in the TMP during the planning phase helps planners envision the scope of the training cycle. The training calendar can be adjusted later, but including it in the planning phase will make for a smooth rollout during the implementation phase.

Identifying instructors is easy for teams developing an in-house program, since the likely candidates have already been involved in the Assessment Phase.

A well-executed Training Management Plan provides structure for and effective training program. A well-maintained TMP will do so for the entire life of the program, and will evolve as the organization’s training needs and goals change. Once the TMP is in place, the next phase can commence.

**Phase 3: Development**

Develop for each topic a “module” of content containing both instructor- and student-facing material such as lesson plans/outlines, lessons (including media and links to web-based elements), learning activities, evaluation materials, and surveys or other feedback tools.

_We have really strong security awareness. We had someone from my team in front of every single employee to provide security training on what they need to do to protect the firm.”_ — CISO at large financial services company
Short animated videos
These can be used to alert users to an issue, and highlight a simple set of actions they can take, something like: https://www.youtube.com/watch?v=Mpsn3Wal_4k. They will focus on addressing user behavior. Users watch the video as a first way to engage with each topic, and can watch it at their leisure. We believe the ability to create and deliver animated video clips is a differentiator because delivery in that format has a major impact on learning and retention. Simply put, people are more likely to remember something if they enjoy watching it.

Online interactive quiz
Each module should include an online, interactive quiz for employees to take following the video, with associated scores and publicly shared rankings. The goal is to “gamify” the learning process to inspire employees to engage. As many people have discovered in their personal lives, doing something extra is sometimes more fun if you’re competing with others. Also note that while we include scores to incent participants to learn, they don’t replace the behavioral metrics discussed below.

Printable checklist
Each module should include a printable checklist for employees to download, print out, and post in their workspace or store for later review.

Online, web-based, and in-person education and communication
In addition to the ad-hoc animated videos, teams should consider developing a short webinar with live online or interactive Q&A, short enough to be scheduled as a “lunch-and-learn” session. The presentation will ideally be pre-recorded and delivered online, with interactive Q&A for a scheduled period following.

Dry runs
Before fully rolling out a program, trainers need to run live sessions and testers need to review all modules, to work out any bugs and make changes while material re-writes and adjustments to the TMP will be less disruptive to the organization. For objectivity, someone other than a module’s developers must test each module. Testing should cover every aspect of a training iteration, from scheduling through testing and feedback.

Ideally, testers will be from the same group the training ultimately targets. They can tell whether certain activities or materials don’t suit the intended learners, in addition to spotting more mundane issues such as links or embedded video that don’t work.
Phase 4: Implementation
Implementation involves more than simply starting training. Determining whether actual training outcomes align with the company’s training goals requires constant evaluation.

Key considerations during the Implementation phase include:
- Participation. Are the targeted learners engaged in the training activities?
- Learning environment. Is someone evaluating the quality of the activities?
- Objectives. Do participants understand the training goals?
- Outcomes. Is the training meeting the training goals?
- Culture. Are leaders visibly participating?

Managers and trainers alike must be familiar with the TMP and understand the training goals laid out in it. Instructors should know their own material and also be familiar with the other course material. Since all instructor material is available in the TMP, instructors should become comfortable with the entire course. Master instructors should be able to sub any other instructor on any given module.

Implementation is a rolling process more than an event. Testing during development does not eliminate the need for constant in-course evaluation. Good leaders foster an environment wherein trainers can critically assess materials procedures. Are failure rates too high (or too low)? Are test completion times too long/too short? Answering these questions will marry effective training to realistic goals.

Phase 5: Ongoing support
It is important enterprises provide employees ongoing support to maintain engagement. Depending on the systems a company deploys (e.g. SAP JAM), this support may be in the form of community engagement and involvement. Again, some third-party companies will help with engagement and involvement.

Repetition in the training program will instill positive habits. “We’ve scared the crap out of all of our employees” says one CSO at a midsize financial services company. “Anyone is afraid to do things without talking to us first. We set a very good precedent. We do training every year.”

Third-Party Awareness Training Vendors
Many third-party companies offer “cybersecurity awareness and compliance” programs. Many provide off-the-shelf packages; those engaging such services should make sure these are “fully customizable.” Moreover, the company should offer
support for those customizing the materials—explicitly offer to help the security team develop custom modules.

Other things to look for in third-party companies are tools such as phishing assessment software, fully hosted web-based content delivery, and tracking metrics. Well-known companies such as Symantec, the InfoSec Institute, and the SANS Institute offer security awareness training. Others include KnowBe4, Inspired Learning, and the Center for Development of Security Excellence (cdse.org). Most of these provide a variety of products and services including training modules.

Vulnerability assessment services providers may go beyond offering awareness assessment quizzes and tools and attempt various forms of social engineering and workplace snooping, to see how “active” the awareness is.

Conclusion and Recommendations
Tech companies continually develop ever-more sophisticated defenses against increasingly sophisticated cybersecurity threats. Despite deployment of multiple overlapping defenses, companies of all sorts and sizes continue to fall victim to phishing and other attacks at an alarming rate. Investing in the best security technology while skimping on training is doomed to failure because virtually no company is immune to human error.

IT security teams can help change a company’s awareness culture with a solid training program. Developing and maintaining a customized, flexible security awareness training program requires leadership buy-in and will involve every member of the company.

To succeed, security professionals involved in the effort must

• Assess the company’s needs and develop training goals and decide whether to train in-house or to involve a reputable third-party training vendor
• Plan a comprehensive awareness training program
• Develop and test a set of custom training modules
• Implement the plan and immediately begin assessing effectiveness
• Monitor and maintain the program by regularly gathering feedback and updating content.
Appendix A: Nemertes Security Maturity Model

As with all Nemertes’ Maturity Models, our Security Maturity Model comprises four tiers of maturity: Unprepared, reactive, proactive, and anticipatory. (Please see Figure 4.)

<table>
<thead>
<tr>
<th>Level</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 0 (Unprepared)</td>
<td>Lacking necessary information to take effective action; unaware of or unable to respond to current or emerging issues</td>
</tr>
<tr>
<td>Level 1 (Reactive)</td>
<td>Have basic platforms and structures to react to business requirements; but cannot proactively prevent problems from arising</td>
</tr>
<tr>
<td>Level 2 (Proactive)</td>
<td>Have platforms, structures, and organizational processes to proactively address current issues and challenges</td>
</tr>
<tr>
<td>Level 3 (Anticipatory)</td>
<td>Have platforms, structures, and organizational processes to proactively address future issues and challenges</td>
</tr>
</tbody>
</table>

**Figure 4: The Nemertes Maturity Model**

**Level 0: Unprepared**
An unprepared organization is one that lacks the tools, processes, people, and most importantly, the knowledge to respond effectively to challenges (let alone deal with them proactively). We deliberately rate this as a “zero” (rather than using more positive terminology) because an organization performing at this level is quite literally failing its most basic charter.
Level 1: Reactive
A reactive organization is performing better, but not by much. As implied by the name, it can respond and react to business requirements, but it’s effectively in “order-taker” mode: the responsibility for defining requirements rests entirely with the business.

Level 2: Proactive
Most organizations aspire to move beyond reactive to proactive. Proactive organizations can not only respond to requests, they can guide the business in making those requests. That is, they’re solving the “problem behind the problem”—the real business issue that’s motivating the request.

Level 3: Anticipatory
But proactive isn’t the highest level of maturity. Ideally, an organization will operate in “anticipatory” mode, meaning that it has the tools, processes, and insight to address not just present but future issues. An anticipatory information security organization might, for instance, have in place a full strategy for protecting Internet of Things (IoT) infrastructure—even before the infrastructure is deployed, or the business need for it is determined.

In a nutshell, an unprepared organization can have minimal positive impact on the enterprise it serves. (Please see Figure 5.) In fact, the impact is largely negative.
(equipment failures, outages, and breaches). A proactive or anticipatory organization, in contrast, can have a strongly positive impact on the enterprise. An anticipatory technology organization is actually a critical foundation for digital transformation.

**Maturity Model Elements**

To assess a cybersecurity organization’s maturity, we looked at several organizational and operational elements. (Please see Figure 6.)

<table>
<thead>
<tr>
<th>Component</th>
<th>Level 0: Unprepared</th>
<th>Level 1: Reactive</th>
<th>Level 2: Proactive</th>
<th>Level 3: Anticipatory</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Budgeting and Investment</strong></td>
<td>No defined security budget</td>
<td>Security budget exists</td>
<td>Benchmark-based: based on comparisons with like organizations and/or with other tech or business spend</td>
<td>Risk-based: start with risk to business, and develop budget for risk mitigation accordingly</td>
</tr>
<tr>
<td><strong>Process for Setting Budget</strong></td>
<td>Ad-hoc: make individual cases based on perceived need</td>
<td>Framework-based: based on external framework</td>
<td>One-hop: CISO is one hop away from senior business executive (CEO, CFO, CIO)</td>
<td>Direct: CISO reports directly to senior business executive (CEO, CFO, CIO)</td>
</tr>
<tr>
<td><strong>Organization</strong></td>
<td>No CISO: highest level of security professional is director or manager</td>
<td>Multiphop: CISO is 2 or more steps down from business (e.g., reports to VP of technology then to CIO then to business)</td>
<td>Both IT and business proactively reach out to InfoSec</td>
<td>Both IT and business consider InfoSec issues even in the absence of InfoSec professionals</td>
</tr>
<tr>
<td><strong>Interaction with Business</strong></td>
<td>InfoSec must proactively reach out to IT and business</td>
<td>IT proactively reaches out to InfoSec, but business does not</td>
<td>Both IT and business proactively reach out to InfoSec</td>
<td>Both IT and business consider InfoSec issues even in the absence of InfoSec professionals</td>
</tr>
<tr>
<td><strong>Security Technology</strong></td>
<td>Big Rock: Primarily procure preferentially from 2-3 strategic technology partners (not security-specific)</td>
<td>Best-in-Breed: Primarily select products based on feature-functionality, not provider relationship</td>
<td>Ecosystem: Primarily procure products based on degree of integration with existing or planned environment</td>
<td>Custom: Work directly with emerging vendors to shape capabilities; may include incubators or investments</td>
</tr>
<tr>
<td><strong>Procurement Strategy</strong></td>
<td>None defined</td>
<td>Defined but revisit less often than annually</td>
<td>Defined and revisit annually (or more frequently)</td>
<td>Defined and revisit annually (or more frequently)</td>
</tr>
<tr>
<td><strong>Security Architecture</strong></td>
<td>None defined</td>
<td>Defined but revisit less often than annually</td>
<td>Defined and revisit annually (or more frequently)</td>
<td>Defined and revisit annually (or more frequently)</td>
</tr>
<tr>
<td><strong>Security Roadmap</strong></td>
<td>None defined</td>
<td>More than 5 years</td>
<td>More than three years</td>
<td>One year or less</td>
</tr>
<tr>
<td><strong>Security Roadmap Planning Horizon</strong></td>
<td>None</td>
<td>More than 5 years</td>
<td>More than three years</td>
<td>One year or less</td>
</tr>
</tbody>
</table>

**Figure 6: Elements of the Maturity Model**

**Bellwether Technologies: Definition**

Bellwether technologies are technologies that successful organizations adopt earlier than other organizations. They serve as “markers” for mature organizations, for two main reasons.

First, companies that deploy them early have a strategic advantage over those who wait, because these technologies typically deliver unprecedented capabilities. They may deliver previously impossible capabilities (such as protecting endpoint applications from launching attacks by running them in micro containers) or
dramatically reduce manual effort and operational costs by automating previously manual capabilities (such as leveraging machine learning to weed out the 3-5 true security events from hundreds of false positives).

Second, these technologies generally require a high degree of maturity from which to deploy and gain benefits. That is, behavioral threat analytics (one type of bellwether technology) requires the “table stakes” of solid firewalling, logging, and monitoring. That said, not all technologies are right for all organizations or vertical industries. Some companies are too small or homogeneous to benefit from each bellwether technology.

Overall, these bellwether technologies correlate with maturity in the following way: unprepared (level 0) security organizations are considerably less likely to be using, assessing, or even considering them; reactive (level 1) security organizations are more likely to be assessing them or considering deployment in 2018 or beyond; proactive (level 2) security organizations are more likely to be planning deployment in 2017; and anticipatory (level 3) organizations are more likely to have them implemented already.

Cybersecurity Bellwether Technologies
The cybersecurity bellwether technologies we tracked included the following:
- **Cloud security and Cloud Access Security Brokers (CASB):** Premise or cloud based software that automatically detects cloud usage by employees, assesses business and technical risk, and enforces policies.
- **Endpoint security:** Software that protects endpoints from malware, using a variety of mechanisms (e.g. microsegmentation).
- **Behavioral Threat Analytics (BTA):** Software that integrates multiple sources of data (logs, analytics platforms such as Splunk, SIEM) to capture and display anomalous behavior of users, devices, and systems.
- **Application security:** Automated application security testing, including Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), Interactive Application Security Testing (IAST), and Runtime Application Security Testing (RAST).
- **Risk management platforms/suites:** Automated technology that translates infosec vulnerabilities into business risk.
- **Threat, Risk, Compliance (TRC) networks:** Also known as threat intelligence networks, these are subscription-based services that provide users with real-time insight into emergence of threats.
- **Managed and professional services:** Third-party services reviewing logs, managing security equipment (e.g. firewalls) and conducting assessments and testing (e.g. penetration testing).
• **Automation:** Use of tools and technologies (both third-party and homegrown) to automate security processes.

For most technologies, successful security organizations were 100% to 300% more likely to be deploying these technologies today, or by the end of 2016, as compared to security organizations, overall. The one exception was managed and professional services, which were deployed by roughly two-thirds of all organizations, with no significant distinction between successful and less successful organizations.
Appendix B: Methodology

Our objective in this benchmark study was to uncover the best practices of the most effective security teams. We began constructing our hypotheses in November, 2015, and conducted interviews in January, 2016. Our goal in the interview process was to go deep rather than broad, which we accomplished first by limiting the number of verticals and participants, and secondly by asking open-ended questions in order to capture the narrative. We looked at the following:

- Organizational structure
- Budgeting
- Investments
- Procurement
- Security team’s interaction with the business line
- Technical investments
- Other

We began analyzing the data and quantifying our findings in February 2016. In March, we characterized the results in a security maturity model addressing the question, "What makes the best, the best." The Nemertes Security Maturity Model provides reliable guidance for security organizations seeking to enhance their security stance.

Company Size: Revenue

Our participants fell into three size categories: “Midsize,” “Large,” and “Very Large.” (Please see Figure 7.) Very Large companies are those whose annual revenue is upward of $10 billion; large companies are those with annual revenue between $1 billion and $10 billion, and midsize companies have revenue between $300.1 million and $1 billion. Annual revenue among the participants averaged $17.8 billion, with a median annual revenue of $7.2 billion.
More than 85% of the participants we interviewed for this study worked for Large or Very Large companies. There were no small companies (those under 300 million annual revenue) in our study.

**Company Size: Employees**
The majority of our participants (76.5%) worked at Very Large companies having more than 10,000 employees. (Please see Figure 8.) The next largest segment, 17.6% worked for Midsize companies having 251 to 2500 employees, followed by 10.5% working for Large companies having between 2,501 and 10,000 employees. Just under 6% worked in Small companies having 250 or fewer staff. Average employee count among all participants was 30,682 employees, with a median employee count of 20,000.
Participants: By Industry
Nemertes conducted interviews with executives and senior IT leaders at 17 companies or organizations to compile its 2016-2017 Benchmark. (Please see Figure 9.) Participants included: Financial Services Firms (29.4%), Educational and Healthcare organizations (23.6%), Manufacturing (17.6%), and “Other” including media, high-tech professional services, utilities, and hospitality (29.4%).
Participants: By Title
We received feedback from a wide range of decision makers and influencers. The largest percentage, 58.8%, came from Chief Information Security Officers, followed by Directors of Security at 29.4%, and Security Managers, 11.8%. (Please see Figure 10.)
Participants: By IT Culture

Regarding the mix of IT cultures among our participants, we found 47.1% self identified as Aggressive. (Please see Figure 11.) Participants who self-identified as having a Leading/Bleeding Edge IT culture came in at 23.5%. Another 23.5% embraced a Moderate culture, and only 5.9% embraced a Conservative IT culture. The good news is that a higher percentage of participants in the 2016-2017 Security Benchmark identified with Aggressive and Leading/Bleeding Edge IT cultures than in the previous security benchmark, while significantly fewer identified with the Conservative IT Culture.

- Leading/Bleeding Edge—“We view technology as a competitive advantage and strategic differentiator and deploy it 12-18 months ahead of our competitors to create and sustain our competitiveness. IT is highly strategic.”
- Aggressive—“We view technology as a competitive advantage and seek to deploy it ahead of most other organizations. IT is strategic.”
Figure 11: Participants by IT Culture

- Moderate—“We are generally conservative, but make exceptions on a case-by-case basis for specific technologies. IT is somewhat strategic.”
- Conservative—“We deploy technology only when it has been proven to deliver a benefit (usually financial), and generally after it has been widely across other organizations. IT is not strategic.”

If you have further questions about our methodology, please contact research@nemertes.com. Clients, please contact client-services@nemertes.com for any assistance. Those interested in engaging with Nemertes, please contact sales@nemertes.com.

About Nemertes Research: Nemertes Research is a research-advisory and consulting firm that specializes in analyzing and quantifying the business value of emerging technologies. You can learn more about Nemertes Research at our Website, www.nemertes.com, or contact us directly at research@nemertes.com.