Exploring the Shift in Security Responsibility

Charles Weir | Lancaster University
Sammy Migues | Synopsys Inc.
Laurie Williams | North Carolina State University

The Building Security in Maturity Model survey has been tracking software security activity adoption in 211 companies over 12 years. This article explores how organizations should adapt to the latest security challenges.

According to the National Institute of Standards and Technology’s National Vulnerability Database, more security vulnerabilities were disclosed in 2020 than any other year to date, in addition to a 60% rise in cybercrime in 2020 due to the COVID-19 pandemic. However, the growth in cybersecurity spending is expected to slow, and corporate boards are questioning the effectiveness of cybersecurity activities as implemented across enterprises globally. As organizations seek to address mounting cybersecurity risk as efficiently as possible and comply with regulations, a myriad of activities are available for improving software security. However, budgets are closely monitored, and organizations desire guidance on which of many possible software security activities to undertake first and how to structure adoption to be most effective at preventing a breach.

The growing risk of cyber breach is causing many companies to start or evolve a software security initiative (SSI), an organization-wide program to instill, measure, manage, and evolve software security activities in a coordinated fashion. The roles and activities of the SSI fundamentally change software development and the organizational structure of software development teams. The SSI is often sponsored by a senior executive, such as a chief information security officer (CISO) or someone at a similar level (e.g., technology, information, security, risk, and other officers), but is also seen led by senior managers.

A team of security specialists who implement the day-to-day actions of an SSI is often referred to as a software security group (SSG), though the team’s name might also have an appropriate organizational focus, such as application security group or product security group. That SSG may be centralized in corporate or may be a federated collection of people in corporate, engineering, and elsewhere. Some companies also have an extended satellite of interested and engaged developers, architects, software managers, testers, and similar roles embedded in the development organization who share an interest in improving software security. The satellite group members are also security specialists, often acting as security champions.

The goal of this article is to help software managers and security professionals to understand opportunities to improve the impact of security initiatives through an analysis of software security activities performed by SSGs in 211 organizations over a 12-year period. These records relate to the work of more than 675,000 software developers in companies including some of the world’s largest and most security focused.

Companies prefer to adopt new activities based upon understanding their use in organizations similar...
As a result, a good process to identify such opportunities to improve the impact of software security specialists is to base them on the activities of leading companies, such as the 211 organizations in our data set.

The Building Security in Maturity Model Study

Since 2008, a team of researchers, including one of the authors, has been gathering objective data on the use of what are now 121 software security activities by conducting in-depth assessments in companies. These data are used to periodically refresh the study’s data model, and that descriptive model informs organizations on actual efforts observed in functioning SSIs, as opposed to a prescriptive model, which would be used to determine coherence with a preconceived approach. Some example activities include building and publishing security features, using automated tools along with a manual review, and integrating black-box security tools into the quality assurance process. More governance-oriented readers can think of these activities as individual controls to be implemented in a risk-based security rubric.

These 121 software security activities are structured via practices in the Building Security in Maturity Model (BSIMM) software security framework. As shown in Table 1, they are organized into four domains: governance, intelligence, secure software development lifecycle (SSDL) touchpoints, and deployment, such that each domain has three practices (or categories).

Each activity has a unique identifier (including leading letters indicating the practice as indicated in Table 1), name, and description. For example, the “SM1.1 Publish process and evolve as necessary” activity, in the strategy and metrics practice, is summarized as defining a strategy for addressing software security, including goals, roles, and responsibilities as well as communicating it to all stakeholders, and “T1.1 Conduct awareness training,” an activity of the training practice, is summarized as using training courses to promote a culture of software security throughout the organization. All of the BSIMM activities are strategic rather than reactive: activities tend to focus, for example, on being prepared to handle security events and fix vulnerabilities, and these activities accomplish certain goals, but there is not an activity that is simply “fix bugs.”

A prerequisite for undergoing a BSIMM assessment is that an organization must have an SSG. Named participants that have undergone a BSIMM assessment include Microsoft, Qualcomm, SAP, Visa, Citigroup, and PayPal. All of the named organizations are commercial companies—mostly headquartered in the Americas (79%) or Europe (17%)—and at least 55 were in the Forbes Global 2000 list of the world’s largest public companies. The list also includes many trailblazers in large company software security, including 70% of the early members of SAFECode (https://safecode.org/), an early initiative in this field.

Each BSIMM assessment is carried out in cooperation with the organization’s SSG. For each assessment, security professionals, including one author of this article, conduct approximately 20 in-person interviews in which they contextually determine whether each activity is being performed sufficiently for the organization to receive credit, calibrating their decisions against those made for other companies by the pool of experts. The interviews typically include the SSG leader, SSG members, and representatives from the development organization whose roles involve implementing security or are affected by the security processes.

| Table 1. The activity domains. |
|-------------------------------|
| Domain | ID | Practice                          |
|--------|----|-----------------------------------|
| Governance | SM  | Strategy and metrics               |
|         | CP  | Compliance and policy             |
|         | T   | Training                           |
| Intelligence | AM  | Attack models                      |
|         | SFD | Security features and design       |
|         | SR  | Standards and requirements         |
| SSDL touchpoints | AA  | Architecture analysis              |
|         | CR  | Code review                        |
|         | ST  | Security testing                    |
| Deployment | PT  | Penetration testing                |
|         | SE  | Software environment               |
|         | CMVM| Configuration management and vulnerability management |
Companies may go through multiple assessments. From the inception of BSIMM up to 1 April 2020, 141 organizations have gone through one assessment; 42 have gone through two assessments; 18 through three assessments; 7 through four assessments; and three have gone through five assessments.

The interviewers record in a database the company demographic data and which of 121 software security activities were practiced. From these data, the interviewers create a “scorecard” report of an organization’s software security activities, including a comparison with other similar companies, such as those in the same industry vertical.

The resulting highly sensitive data set of scorecard results is a trove of 322 assessments of 211 companies throughout the world over a 12-year period, relating to the work of some 675,000 software developers. We are aware of no similar work of this magnitude in the field of software security.

Since 2009, the BSIMM team has published 11 reports containing a high-level descriptive analysis of that year’s data. Each year, a report is publicly available to those willing to provide contact information; the latest is the BSIMM11 report from 2020. Each report also includes a detailed definition of every activity. From year to year, activity descriptions are refreshed to use current vocabulary and examples, and new activities might be added to the model. To date, no activity has been deleted from the model.

This article takes a different approach to the analysis in those reports, using graphical and longitudinal analyses to pull out further objective results and conclusions as well as specifically examining the activities of the SSG. To preserve confidentiality, non-Synopsys authors of this article had no access to the organization names associated with any particular BSIMM data analyzed.

**Introducing This Study**

In this article, we explore the software security activities performed by the SSG. Effective security requires an additional effort by other organizational roles, especially software developers and executive management, but their activities are out of scope for this article. (Indeed, we previously reported an analysis of the software security activity adoption patterns of software developers.) In this article, we report on both adoption—starting new activities—and the continued usage of activities by the SSG.

To categorize the 121 BSIMM software security activities, we assigned each one as “carried out by the SSG” (called an SSG activity) or not. We also assigned tasks carried out by development teams—including quality assurance and operations staff. Because the SSG is essentially a service organization, we then classified each SSG activity as to whether it benefited software developers, management (including policymakers), or both. For example, the previously mentioned “SM1.1 Publish process and evolve as necessary” is a service for both management and software developers. In this article, we report on both adoption—starting new activities—and the continued usage of activities by the SSG.

To categorize the 121 BSIMM software security activities, we assigned each one as “carried out by the SSG” (called an SSG activity) or not. We also assigned tasks carried out by development teams—including quality assurance and operations staff. Because the SSG is essentially a service organization, we then classified each SSG activity as to whether it benefited software developers, management (including policymakers), or both. For example, the previously mentioned “SM1.1 Publish process and evolve as necessary” is a service for both management and software developers. To ensure objectivity, we used dual thematic coding: two authors first coded the activities independently (Cohen’s kappa = 0.51); compared differences; independently recorded all of the activities; and, finally, agreed on the coding for the few remaining differences.

From the initial set of 121 software security activities, we identified 73 SSG activities with beneficiaries as shown in Figure 1. Only one activity, “AM3.1 Team develops new attack methods,” was assigned as having no beneficiaries outside the SSG team.

**Table 2. The distribution of SSG activities.**

| Governance | Intelligence | SSDL Touchpoints | Deployment |
|------------|-------------|------------------|------------|
| Strategy and metrics | Attack models | Architecture analysis | Penetration testing |
| 10 of 12 | 10 of 11 | 4 of 9 | 2 of 7 |
| Compliance and policy | Security features and design | Code review | Software environment |
| 9 of 11 | 7 of 7 | 5 of 11 | 1 of 10 |
| Training | Standards and requirement | Security testing | Configuration and Vulnerability Management |
| 12 of 12 | 6 of 10 | 2 of 10 | 5 of 11 |
| 31/35 (89%) | 23/28 (82%) | 11/30 (37%) | 8/28 (29%) |

Figure 1. Who benefits from each SSG activity?
framework. The majority of the activities (54 of 73) are in the governance and intelligence domains, for which the SSG was assigned as having 89% and 82% of the activities, respectively.

**Trends in Security Staffing**

Both the SSG and the satellite contain security specialists in an organization. Much of this article focuses on the activities of the SSG and not the satellite because the activities of the latter are not specifically delineated in the BSIMM data. However, the BSIMM demographics and selected practices provide a holistic view of these security specialists. To give context, Table 3 shows median, lower decile, and upper deciles for the sizes of development teams, SSG teams, and satellite in the most recent survey for each of the 211 companies.

We wondered to what extent the increase in need for security is being reflected in staffing levels. To make valid comparisons, we considered only the 111 assessments on the 70 organizations that had more than one assessment. Figures 2 and 3 show changes in SSG and satellite sizes, respectively, over the years in companies that had more than one assessment. Given that the BSIMM is used to measure SSG efforts, we can say with confidence that none of the 70 organizations with more than one assessment abandoned their SSG between assessments unless they also started another one before getting the next assessment. As a requirement, all organizations evaluated had an SSG, so the SSG changes are represented as percentages; note that the small SSG sizes mean that large percentage changes may not reflect large staff changes.

Because all of the figures represented repeat assessments, Figure 2 offers an indication of how well-established SSG teams have responded to changes in the cybersecurity landscape, though we have no information about whether any organizations abandoned their SSG teams in that period. As the circled area on Figure 2 shows, there was a trend of substantial increases in SSG size between 2016 and 2018. Since then, SSG sizes have tended, if anything, to decrease slightly.

Having a satellite, however, is optional for a company assessed by the BSIMM, and, as Figure 3 shows, many organizations either created or abandoned them between surveys. Since 2016, many companies have created new satellite operations, and, latterly, despite false starts in some organizations, we generally see increasing numbers of satellites and an expansion of existing ones (as circled on the chart), encouraging expertise within development teams.

Data on individual activities also shed light on satellite creation. Activity “T3.6 Identify new satellite members through observation” has decreased from 22% in 2012 to less than 1% in 2020. Similarly, activity “SM2.3 Create or grow a satellite” has decreased from 51% in 2012 to 42% in 2020. In the BSIMM11 report, the authors reflect that some activities become a part of the culture, and the SSG may not need to explicitly select satellite members if a good stream of qualified engineers volunteer to assume a satellite role. The assessors also observed that the satellite role is evolving rapidly in engineering-led firms that are embracing DevOps and DevOps modified for security (DevSecOps), where satellite members apply their expertise for the benefit of the organization at large.

**Trends in Activity Adoption**

Figure 4 shows a kernel density estimation plot adoption of activities by the SSG group as seen in the full 211 surveys, expressed as a percentage of the maximum possible (73). The amber line plots the two-year
moving average. The surprising decrease in the moving average between 2012 and 2016 may reflect that the early adopters of the BSIMM survey were among the most enthusiastic and rigorous adopters of software security, while later BSIMM participants tended to be less advanced in software security. As the circled area shows, many assessments in 2016–2017 found relatively low numbers of activities. Reassuringly, from about 2017, we see a gradual increase in the mean percentages of activities found per assessment.

Industrial reports, such as that by Migues,\textsuperscript{7} indicate a rise in “shifting left” and “shifting everywhere” related to applying application security techniques earlier in the software lifecycle and early testing for important characteristics, such as security, quality, compliance, adherence, reliability, resilience, and so on. We hypothesized that these shifts will be observed as a decline in activities done by the SSG, with a corresponding increase in activities done by software developers.

Figure 5 explores this hypothesis. The top two (green and brown) lines show trends in activities by SSGs in service of development teams and management, respectively—as a proportion of their maximums (63 and 31, respectively). The bottom (purple) line shows activities done by developers as a proportion of that maximum (43). The correlated lines in the three areas do not support our hypothesis: as the top line in the highlighted oval shows, we are not seeing a decline in activities done by SSGs for developers; instead, the number is increasing. The bottom two lines in the oval, however, do show a somewhat larger increase in SSG activities for management and an increase in activities done by developers themselves.

We conclude that, after some six years of companies playing “catch-up” with the most security-competent organizations, in the last five years we’re seeing software security moving from requiring just a relationship between security specialists and developers to necessitating relationships between security specialists and a variety of other parts of the company. Security responsibility is not just “shifting left” or “shifting everywhere” in the development process; it is shifting everywhere within the organization. The number of activities in use is now tending to increase in all parts of the company. We can reasonably conclude that many organizations are moving from centralized corporate security teams being the sole arbiters of software security technology choices and use to something more like a shared responsibility or federated model, where different parts of the organization have a responsibility for choices in governance, technology, testing, risk management, cloud security, configurations, and supply chain control.

\begin{figure}
\centering
\includegraphics[width=\textwidth]{figure4}
\caption{The proportion of all possible SSG activities seen over time.}
\end{figure}

\begin{figure}
\centering
\includegraphics[width=\textwidth]{figure5}
\caption{The proportion of possible activities seen in each category.}
\end{figure}
Patterns in Activity Use
While historical trends are useful to know, practices in software development naturally change over time, so practical adopters are most interested in recent data. This section, therefore, considers only activities and changes in the five-year period of 2015–2020.

Figure 6 shows those 37 of the assigned SSG activities that were found in more than 20% of companies during that time, clustered to show the extent to which they are used together. The agglomerative clustering algorithm used here calculates the distance between any two activities to be the ratio of assessments finding both activities to those finding either activity but not both. The algorithm adds further activities to each cluster in such a way as to minimize the largest distance between any two items in a cluster (“complete” clustering).
linkage). Where companies were assessed more than once, only the last assessment was used. Distances are shown on the x-axis; in the y-axis legend, lines separate the clusters found, grayed-out labels show unclustered activities, and the parentheses contain the first letter of the domain (governance, intelligence, SSDL touchpoints, and deployment) and the activity code. Detailed descriptions of each activity can be found in the publicly available BSIMM11 report.5

The top 11 activities in Figure 6 are clustered with each other (yellow cluster), and each is used by at least 61% of the companies. As such, these activities can be considered a proverbial “starter pack” because they are adopted frequently and together. Since the survey covers a good cross section of early adopters of software security and, therefore, much industry “best practice,” we conclude that these are likely to be suitable first steps for other organizations starting an SSI.

The “starter pack” has activities in seven of the 12 practices. Six of these top 11 activities are in the governance domain, three are in the intelligence domain, one is in the SSDL touchpoint domain, and one is in the deployment domain. The predominance of starter pack activities in the governance domain is indicative of organizations with predominately a top-down, governance-driven approach to software security in which the SSG defines rules that engineers must follow. We believe the emerging shift-left and shift-everywhere approaches and perceived need for increased software resilience in the face of increasing security breaches is leading toward an emerging bottom-up, engineering-driven security culture, which may become more prominent in future assessments.

Figure 6 also shows that specific kinds of activities tend to be found together. The clusters are labeled on the diagram as representing the following:

- evangelism by SSGs to development teams
- risk-based decision support
- support for compliance activities
- activities to promote executive awareness
- training activities
- promoting satellites and security champions among developers
- supporting tool mentors and providing evidence for them to use.

These activities can be considered a proverbial “starter pack” because they are adopted frequently and together.

We conclude that the adoption of SSG activities tends to be driven by corporate priorities: some organizations are most focused on compliance, others on distributing security knowledge by building up a satellite of developer champions, and some are beginning to place effort—and, perhaps, responsibility—for software security within engineering. These patterns are different from developer adoption of software security activities, which tends to be driven by non-SSG champions in particular roles.5

Next, we explored how SSG activities have changed in the five-year period. Tables 4 and 5 compare activities in 2015–2016 with those for 2019–2020, including the beneficiary and domain of each activity. Table 4 shows the 10 activities that have shown the greatest average increase. For example, a newly popular activity is “SR2.2 Create standards review board,” which has increased by 25 percentage points: from 27% to 52% adoption. Five of these top 10 activities are from the governance domain, four are from the intelligence domain, and one is from the SSDL touchpoints domain. This is consistent with the distribution of SSG activities shown in Table 2 but may also reflect an increase in externally imposed governance, regulations, and standards. We observe that three of these “top 10” support management, five support management and developers, and two support only developers—a distribution more evenly loaded toward helping management when compared with the distribution in Figure 1.

The four activities from the intelligence domain are all related to standards and requirements. Only one of the increased activities comes from either of the SSDL touchpoint or deployment domains—those most often done by software engineering teams. These top 10 substantiate a continuing emphasis on governance-led efforts.

Table 5 shows the corresponding decreased activities over the same period. The top decrease was an 11% decline, while seven of the 10 decreases were of 2% or less—in the context of an overall increase in activity adoption, as shown in Figure 4. Four are from the governance domain, four are from the intelligence domain, and the top two largest decreases come from the SSDL touchpoints domain. We observe that five of these “top 10 decreases” support developers, two support management and developers, and...
three support only managers—a distribution skewed toward a decrease in the SSG helping developers. For example, the results indicate decreases in attack models and code review—which may indicate these practices are no longer done by the SSG but, instead, by the development teams.

This pattern again appears to be less of a “shift left,” in which security testing and analysis are done earlier in the development cycle, and more a shift of responsibility: security is moving from being the sole responsibility of a separate security team to being something of a responsibility for everyone, especially developers. Indications are that the role of the SSG is moving from being solely the introducer and justifier of good software security to providing a security support service to every aspect of software product delivery.

What Influences Adoption Rates?
We explored how the number of SSG activities varied with different aspects of each company assessed. We found little correlation with companies’ industry sectors but did find a previously unexpected link to the number of security specialists involved. Figure 7 plots the number of activities adopted in assessments since 2015 (as a proportion of the maximum 73 assigned SSG activities) against the combined SSG and satellite size (log scale). It shows a strong correlation, represented by the Pearson R statistics, the straight amber line, and its shaded 95% confidence limits.

Table 6 compares this with correlations calculated against several other possible size attributes of each company, including developer/security staff ratios: all show a linear relationship, but only the regression in Figure 7 explains as much as 69% of the variation. Though we had not predicted the correlation prior to the analysis, the tiny p value means we can trust this result as statistically sound.

What Should We Do?
Returning to the goal of this article, to help software managers and security professionals understand opportunities to improve the impact of security initiatives, we observe that, given the trailblazing nature of the companies surveyed, their approaches are likely to be good ones to follow. We can therefore identify several suggestions:

- Focus initially on the 11 “starter pack” activities, shown at the top of Figure 6. The emphasis on governance activities leverages the increasing pressure on

| Use in 2019–2020 (%) | Change (%) | Description | For Management | For Developers | Domain |
|----------------------|------------|-------------|----------------|----------------|--------|
| 52                   | 25         | Create standards review board (SR2.2) | | | Intelligence |
| 37                   | 25         | Create SLA boilerplate (SR2.5) | | | Intelligence |
| 37                   | 25         | Have software security resources in onboarding (T1.8) | | | Governance |
| 72                   | 20         | Publish SW sec process and evolve it (SM1.1) | | | Governance |
| 24                   | 19         | Provide training for vendors/outsource workers (T3.2) | | | Governance |
| 69                   | 18         | Create security standards (SR1.1) | | | Intelligence |
| 24                   | 18         | Control open source risk (SR3.1) | | | Intelligence |
| 61                   | 18         | Executive awareness of compliance/privacy needs (CP2.5) | | | Governance |
| 63                   | 17         | Educate executives (SM1.3) | | | Governance |
| 40                   | 17         | Assign tool mentors (CR1.7) | | | SSDL touchpoints |
companies to get at least minimal security governance in place, providing a framework for developers and other groups.

- Create and build up a “satellite” of interested technical staff to be as extensive as possible because the adoption of security activities certainly tends to increase with greater total security staff sizes (Figure 7).

- Have the SSG leave the technical aspects of software security to the project development teams, supported by this satellite of security-aware technical staff, and, instead, focus on support for cross-organization issues such as onboarding, standards, management processes, and the appropriate use of open source software (Tables 4 and 5).

### Table 5. The 10 largest decreases.

| Use in 2019–2020 (%) | Change (%) | Activity Description | For Management | For Developers | Domain |
|-----------------------|------------|----------------------|----------------|---------------|--------|
| 9                     | –11        | Make top n bugs list and use it to drive change (CR2.7) |                |               | SSDL touchpoints |
| 53                    | –4         | SSG performs opportunistic code review (CR1.2) |                |               | SSDL touchpoints |
| 7                     | –4         | Collect and publish attack stories (AM2.6) |                |               | Intelligence |
| 4                     | –2         | Attack patterns/abuse cases tied to attackers (AM2.1) |                |               | Intelligence |
| 12                    | –2         | ID metrics and use them to drive budgets (SM3.3) |                |               | Governance |
| 57                    | –2         | Engage SSG with architecture (SFD1.2) |                |               | Intelligence |
| 64                    | –2         | Provide software security awareness training (T1.1) |                |               | Governance |
| 35                    | –1         | Security signoff for compliance-related risk (CP2.2) |                |               | Governance |
| 7                     | –1         | Communicate SW sec standards to vendors (SR3.2) |                |               | Intelligence |
| 5                     | –1         | Run external marketing program (SM3.2) |                |               | Governance |

### Table 6. The correlation of adoption rates with (log of) different company attributes.

| Attributes                        | Pearson Correlation |
|-----------------------------------|---------------------|
| Combined SSG and satellite size   | $r = 0.69, p = 2.9e-28$ (n = 190) |
| SSG size                          | $r = 0.56, p = 4.6e-17$ (n = 189) |
| Development size                  | $r = 0.49, p = 1.3e-12$ (n = 190) |
| Developers per SSG and satellite  | $r = 0.25, p = 0.00063$ (n = 190) |
| Developers per SSG                | $r = -0.14, p = 0.057$ (n = 190) |
We speculate that this finding requires two different sets of skills in security specialists. The security skills measured by qualifications, such as the “Certified Secure Software Lifecycle Professional”—including expertise in areas, such as penetration testing, cloud security, threat modeling, and a detailed knowledge of possible vulnerabilities and vulnerability management—are now likely to be more important within members of the satellite. These skills can then be less important in SSG members, who will need negotiation abilities, software architect skills, training capabilities, and general evangelism skills as well as an ability to define, create, and manage through useful metrics.

For management, increasingly, trustworthiness in cybersecurity is becoming an important corporate asset, and much is at stake. Based on the experience of many large company adopters of security, we conclude that the combination of concentrating on an initial “starter pack” of activities, building up a satellite within the development teams, and having the SSG focus on cross-organizational issues offers an excellent way forward.

Acknowledgments
This research was partially funded through the U.K. PETRAS National Center of Excellence for Internet of Things Systems Cybersecurity under Engineering and Physical Sciences Research Council grant EP/S035362/1 and U.S. National Science Foundation grant 1909516. The authors acknowledge the contribution of Mike Ware, formerly senior director of technology at Synopsys.

References
1. “NIST security vulnerability trends in 2020: An analysis,” Redscan, 2020.
2. J. Firch, “10 cyber security trends you can’t ignore in 2021,” PurpleSec, 2021. [Online]. Available: https://purplesec.us/cyber-security-trends-2021/ (Accessed: Feb. 25, 2021).
3. P. Proctor, “The urgency to treat cybersecurity as a business decision,” Gartner Group, 2021.
4. S. Migues, J. Steven, and M. Ware, “BSIMM11,” BSIMM Rep., 2020. [Online]. Available: https://www.bsimm.com/content/dam/bsimm/reports/bsimm11.pdf
5. C. Weir, S. Migues, M. Ware, and L. Williams, “Infiltrating security into development: Exploring the world’s largest software security study,” in Proc. 29th ACM Joint Eur. Softw. Eng. Conf. Symp. Found. Softw. Eng. (ESEC/FSE ’21), Aug. 23–28, 2021, vol. 1, no. 1, p. 11.
6. G. A. Moore, Crossing the Chasm: Marketing and Selling Disruptive Products to Mainstream Customers. New York, NY, USA: Harper Collins, 2009.
7. S. Migues, “Why ‘shift everywhere’ is the new ‘shift left’ for software testing,” Forbes Magazine, 2021. [Online]. Available: https://www.forbes.com/sites/forbestechcouncil/2021/07/16/why-shift-everywhere-is-the-new-shift-left-for-software-testing/ (Accessed: Aug. 17, 2021).
8. F. Murtagh and P. Contreras, “Algorithms for hierarchical clustering: An overview,” Wiley Interdiscip. Rev. Data Min. Knowl. Discov, vol. 2, no. 1, pp. 86–97, 2012, doi: 10.1002/widm.53.
9. J. M. Haney and W. G. Lutters, “Skills and characteristics of successful cybersecurity advocates,” in Proc. Workshop on Security Inf. Workers—SIW, 2017.

Charles Weir is a research fellow at Lancaster University, Lancaster, LA1 4WA, England. His research interests include running software development projects and helping development teams improve software security. Weir received a Ph.D. in philosophy from Lancaster University. He is a Member of IEEE. Contact him at c.weir1@lancaster.ac.uk.

Sammy Migues is a principal scientist at Synopsys, Inc., Herndon, Virginia, 20171, USA; he is a creator of the Building Security in Maturity Model and has been its maintainer and data analyst since inception. His research interests include software security, cybersecurity programs, DevSecOps, metrics, and risk management. Migues received a master’s degree in liberal studies, interdisciplinary technology, and information security from Eastern Michigan University. Contact him at samuel.migues@synopsys.com.

Laurie Williams is a distinguished university professor at North Carolina State University, Raleigh, North Carolina, 27695, USA. Her research focuses on software security and software process. Williams received a Ph.D. in computer science from the University of Utah. She is a Fellow of IEEE and the Association for Computing Machinery. Contact her as lawilli3@ncsu.edu.