Exploring the Shift in Security Responsibility

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

As software security becomes vital, how should organizations adapt to the challenge? This article explores the BSIMM survey of software security activity adoption in 211 companies over 12 years. It identifies a starter pack of 11 widely adopted activities, and justifies a 'Satellite' of security expertise embedded within development teams.

According to the NIST National Vulnerability Database , more security vulnerabilities were disclosed in 2020 than any other year to date [1], in addition to a 600% rise in cybercrime in 2020 due to the Covid-19 pandemic [2]. 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 [3]. As organizations seek to address mounting cybersecurity risk as efficiently as possible and to comply with regulations, a myriad of activities is 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 organizations 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 organizations. The SSI is often sponsored by a senior executive, such as a Chief Information Security Officer (CISO) or similar level (e.g., technology, information, security, risk, and other officers), but is also seen led by senior managers [4].

A team of security specialists who implement the day-to-day actions of an SSI are 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 organizations 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 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 [5].

Organizations prefer to adopt new activities based upon understanding their use in organizations similar to their own [6]. 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 organizations, such as the 211 organizations in our dataset.

The BSIMM Study

Since 2008, a team of researchers, including one of the authors, has been gathering objective data on the use of what is now121 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

Table 1: Activity Domains

Domain	Practice
Governance	Strategy & Metrics (SM) Compliance & Policy (CP) Training (T)
Intelligence	Attack Models (AM) Security Features & Design (SFD) Standards & Requirements (SR)
SSDL Touchpoints	Architecture Analysis (AA) Code Review (CR) Security Testing (ST)
Deployment	Penetration Testing (PT) Software Environment (SE) Configuration Management & Vulnerability Management (CMVM)

informs organizations on actual efforts observed in functioning SSIs, as opposed to prescriptive models used to determine coherence with a pre-conceived approach. Some example activities include: build and publish security features; use automated tools along with a manual review; and integrate black-box security tools into the quality assurance process. The more governance-oriented reader 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 (SSF). 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 (denoting the Practice category), name, and description. For example, the *[SM1.1] Publish process and evolve as necessary* activity, in the Strategy & Metrics practice is summarized as defining a strategy for addressing software security including goals, roles, and responsibilities, and 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 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 that these activities accomplish certain goals, but there isn't 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 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 [5].

Each BSIMM assessment is carried out in cooperation with the organization's SSG. For each assessment, security professionals, including one author of this paper, 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 organizations 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 whose roles are affected by the security processes. Organizations may go through multiple assessments. From the inception of BSIMM up to April 1, 2020, 141 organizations have gone through 1 assessment; 42 organizations have gone through 2 assessments; 18 through 3 assessments; 7 through 4 assessments; and 3 have gone through 5 assessments.

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

The resulting highly-sensitive dataset 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 eleven 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 [4]. 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 analysis to pull out further objective results and conclusions, and specifically examining the activities of the SSG. To preserve confidentiality, non-Synopsys authors of this paper 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 additional effort by other organizational roles, especially software developers and executive management, but their activities are out of scope for this paper (indeed, we previously reported an analysis of the software security activity adoption patterns of

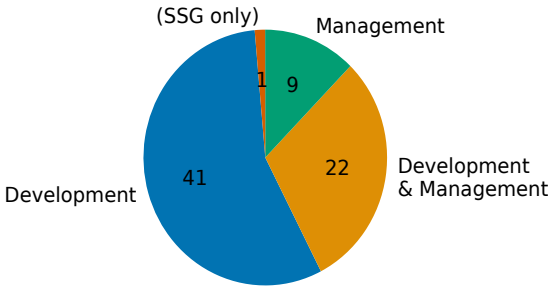

Figure 1: Who benefits from each SSG activity?

software developers [4]). In this paper, we report on both *adoption*, starting new Activities, and continued *usage* of Activities by the SSG.

To categorize the 121 BSIMM software security Activities, we assigned each activity as 'carried out by SSG' (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 the activity benefitted 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); then compared differences; then independently re-coded all 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 shows the distribution of SSG Activities to the 4 domains and 12 practices of the BSIMM 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.

Table 2: 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 & Policy	Sec. Features & Design	Code Review	Software Environment
9 of 11	7 of 7	5 of 11	1 of 10
Training	Standards & Requirement	Security Testing	Config. & 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%)

Table 3: Team Size Distributions

	Low 10%	Median	Top 10%
Dev. team size	100	800	7500
Satellite size	0	0	78
SSG team size	1	6	35

Trends in Security Staffing

Both the SSG and the Satellite are security specialists in an organization. Much of this paper focuses on the Activities of the SSG and not the Satellite because the activities of the Satellite 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. Figure 2 and Figure 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 the figures represent *repeat* assessments, Figure 2 offers an indication of how the sizes of well-established SSG teams have varied in response to changes in the cybersecurity landscape.

Since all the figures represented *repeat* assessments, Figure 2 offers an indication of how well-established SSG teams have responded to the changes in the cybersecurity landscape, though we have no information whether any

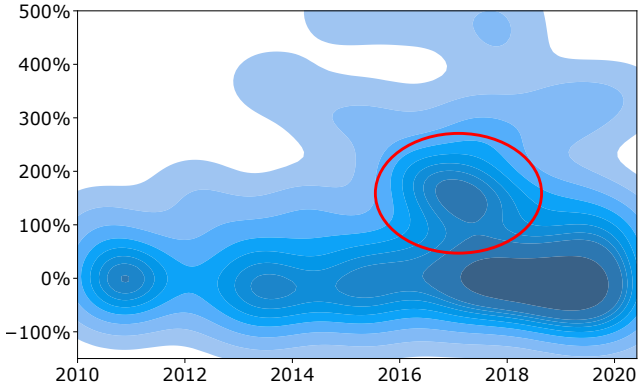

Figure 2: Increments in SSG size in repeat surveys

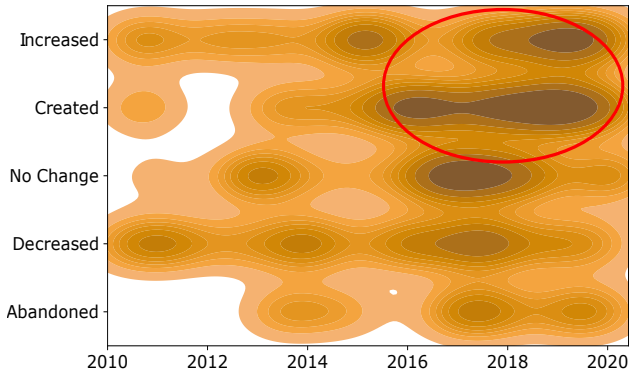

Figure 3: Satellite size changes in repeat surveys

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 organizations have created new Satellite operations, and latterly, despite false starts in some organizations, we generally see increasing numbers of Satellites and expansion of existing ones (as circled on the chart), encouraging expertise within development teams.

Data on individual activities also sheds 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 [5]. Similarly, activity *[SM2.3] Create or grow a satellite* has decreased from 51% in 2012 to 42% in 2020. In the BSIMM11 report [5], the authors reflect that some activities become a part of the culture, and that 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 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 (KDE) 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 2-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, whilst later BSIMM participants tended to be less advanced in software security. As the circled area shows, many assessments in 2016-17 found relatively low numbers of activities. Reassuringly, from about 2017 we see a gradual increase in the mean percentages of Activities found per assessment.

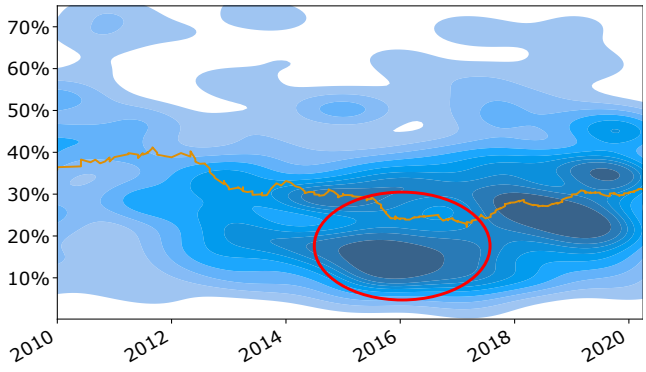

Figure 4: Proportion of all possible SSG activities seen over time

Industrial reports, such as [7], indicate a rise in 'shifting left' and 'shifting everywhere' related to applying application security techniques earlier in the software life cycle and to early testing for important characteristics such as security, quality, compliance, adherence, reliability, resilience, and so on. We would hypothesize that these shifts will be observed as a decline in Activities done by the SSG, with a corresponding increase in Activities done by the software developers. Figure 5 explores this hypothesis. The top two (green and brown) lines show trends in Activities by SSG in service of development teams and management, respectively—as a proportion of their maximums (63, 31). 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 highlighting oval shows, we are not seeing a decline in Activities done by SSG 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 requiring relationships

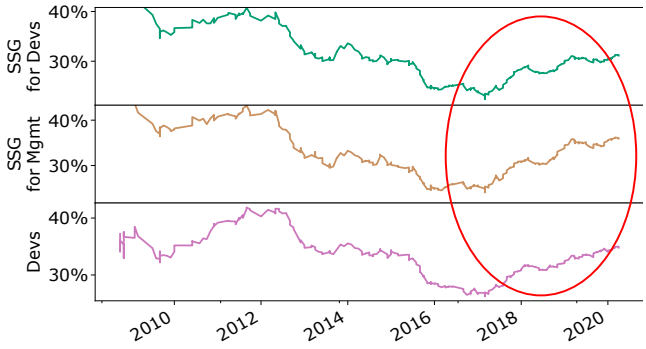

Figure 5: Proportion of possible activities seen in each category

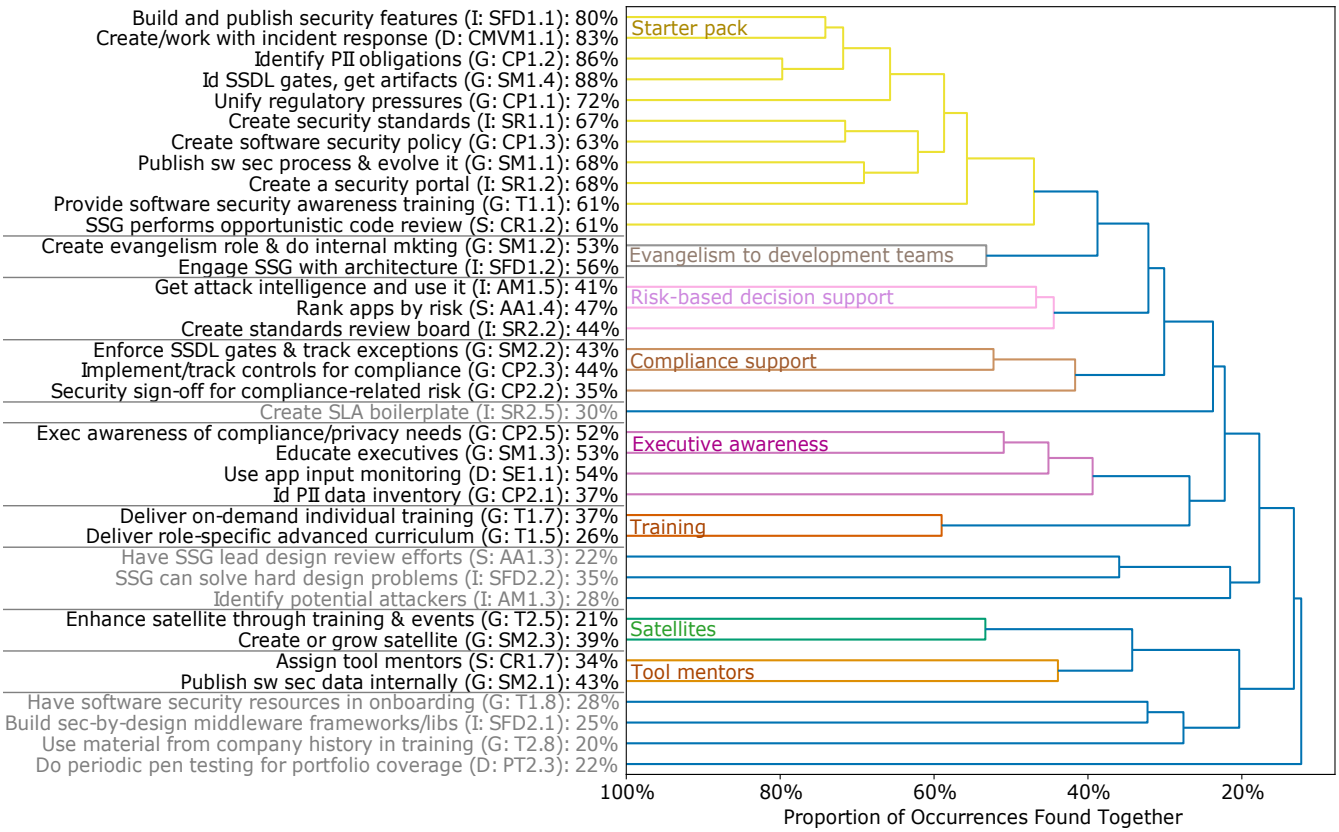

Figure 6: Clusters of Frequently Adopted Activities

between security specialists and a variety of other parts of the organization. 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 organization.

We can reasonably conclude that many organizations are moving from centralized corporate security teams being the sole arbiter of software security technology choices and use, to something more like a shared responsibility or federated model where different parts of the organization have responsibility for choices in governance, technology, testing, risk management, cloud security, configurations, and supply chain control.

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 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 [8] used here calculates the distance between any two activities to be the ratio of assessments finding both activities to assessments 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 any cluster ('complete' 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, greyed out labels show unclustered activities; and the parentheses contain the first letter of the Domain (**G**overnance, **I**ntelligence, **S**SDL Touchpoints, **D**eployment) and the Activity Code. The detailed descriptions of each Activity can be found in the publicly-available BSIMM11 report [4].

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 a software security initiative.

The 'starter pack' has Activities in 7 of the 12 practices. Six of these top 11 activities are in the Governance domain, three in the Intelligence domain, one in the SSDL Touchpoint domain, and one is in the Deployment domain. The

Table 4: Ten Greatest Increases

Use in 2019-20	Change	Description	For M'gement	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 & evolve it (SM1.1)			Governance
24%	19%	Provide training for vendors/out-source workers (T3.2)			Governance
69%	18%	Create security standards (SR1.1)			Intelligence
24%	18%	Control open-source risk (SR3.1)			Intelligence
61%	18%	Exec awareness of compliance/privacy needs (CP2.5)			Governance
63%	17%	Educate executives (SM1.3)			Governance
40%	17%	Assign tool mentors (CR1.7)			SSDL Touchpoints

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 activity tend to be found together. The clusters are labelled on the diagram as representing:

- Evangelism by SSG to development teams;
- Risk-based decision support;
- Support for compliance activities;
- Activities to promote executive awareness;
- Training activities;
- Promoting Satellites and security champions amongst developers; and
- Supporting tool mentors and providing evidence for them to use.

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], and might require future recalibration between centralized and engineering efforts.

Next, we explored how SSG Activities have changed in the five-year period. Table 4 and Table 5 compare activities in 2015-2016 with activities for 2019-2020, including the beneficiary and the domain of the activity. Table 4 shows the ten activities that have shown the greatest average increase. For example, a newly popular activity is *"Create standards review board (SR2.2)"*, which has increased by 25 percentage points: from 27% adoption to 52% adoption. Five of these top ten activities are from the Governance domain, four are from the Intelligence domain, and one is from the 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.

Five of these top ten activities are from the Governance domain, four are from the Intelligence domain, and one is from the SSDL Touchpoints domain. This Domain distribution is consistent with the distribution of SSG activities shown in Table 1 but may also reflect an increase in externally-imposed governance, regulations, and standards. The four from the Intelligence domain are all related to standards and requirements. Only one of the increased Activities come from either of the SSDL Touchpoint or Deployment domains, the domains most often done by software engineering teams. These top ten 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 7 of the 10 decreases were for 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 of the top 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

Table 5: Ten Largest Decreases

Use in 2019-20	Change	Activity	For M'gement	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 sign-off 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

SSG helping developers. For example, results indicate decreases in attack models and code review – which may indicate these practices are no longer done by SSG but instead by the development teams.

This pattern again appears less a 'shift left', in which security testing and security 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 introducers and justifiers 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.

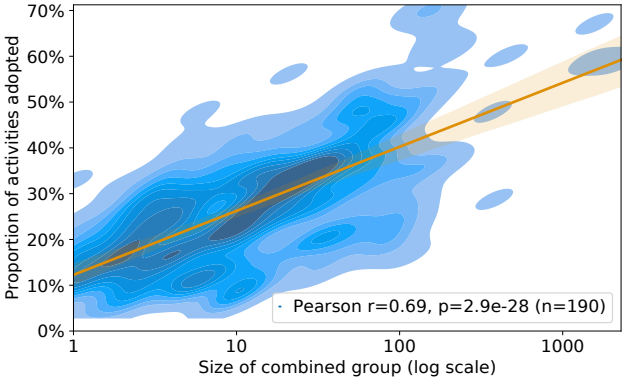

Figure 7: Adoption by combined SSG and Satellite size

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 Figure 7's regression explains as much as 69% of the variation. Though we had not predicted the correlation prior to 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 to 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:

1. To 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 companies to get at least minimal security Governance in place, providing a framework for developers and other groups.
2. To create and build up a 'Satellite' of interested technical staff to be as extensive as possible, because the adoption

Table 6: Correlation of Adoption Rates with (log of) Different Company Attributes

Attribute	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)*
Devs. per SSG&Satellite	*r=0.25, p=0.00063 (n=190)*
Devs. per SSG	*r=-0.14, p=0.057 (n=190)*

of security Activities certainly tends to increase with increasing total security staff sizes (Figure 7).

3. To 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 to focus on support for cross-organization issues such as onboarding, standards, management processes and the appropriate use of open source software (Table 4 and Table 5)

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' (CSSLP)—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 ability, software architect skills, training ability, and general evangelism skills [9], as well as an ability to define, create, and manage through useful metrics.

For management, increasingly trustworthiness at cybersecurity is becoming an important corporate asset [3], 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 SSG focus on cross-organizational issues, offers an excellent way forward.

Acknowledgement

This research was partially funded through the UK PETRAS National Centre of Excellence for IoT Systems Cybersecurity under EPSRC grant number EP/S035362/1; and through the US National Science Foundation grant 1909516.

The authors acknowledge the contribution of Mike Ware, formerly Senior Director of Technology at Synopsys.

References

[1] Redscan, "NIST Security Vulnerability Trends in 2020: An Analysis," 2020.

[2] J. Firch and PurpleSec, "10 Cyber Security Trends You Can't Ignore In 2021," 2021. [Online]. Available: https://purplesec.us/cyber-security-trends-2021/. [Accessed: 25-Feb-2021].

[3] P. Proctor and Gartner Group, "The Urgency to Treat Cybersecurity as a Business Decision," 2021.

[4] S. Migues, J. Steven, and M. Ware, "BSIMM11 Report," 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 *Proceedings of the 29th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE '21), August 23-28, 2021, Athens, Greece*, 2021, vol. 1, no. 1, p. 11.

[6] G. A. Moore, *Crossing the Chasm: Marketing and Selling Disruptive Products to Mainstream Customers*. 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: 17-Aug-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.

[9] J. M. Haney and W. G. Lutters, "Skills and Characteristics of Successful Cybersecurity Advocates," in *Workshop on Security Information Workers - SIW*, 2017.

Charles Weir is a Research Fellow at Lancaster University. With a background running software development projects, he now researches helping development teams improve software security.

Sammy Migues is a Principal Scientist at Synopsys. Sammy is a creator of the BSIMM and has been its maintainer and data analyst since inception.

Laurie Williams is a Distinguished University Professor at North Carolina State University. Her research focuses on software security and software process.