Research Note

Life-Critical Applications and Serverless Computing

Developer Usability vs. Public Risk in AWS Lambda

Kate Schenot

Published: April 2018
Written: February 2018

Keywords: Emergency Services; Critical Infrastructure; Serverless Computing; Cloud Technologies; Amazon Web Services; Lambda; First Respondents

Abstract: This paper discusses the risk arising from the emerging intersection of public safety, emergency response technology, the Internet of Things, and computerless servers such as Amazon Web Services' Lambda. The critical question is: When a product such as Lambda poses such powerful possibilities in the public sphere, at what point is developers' ease-of-use a liability for the people?

Public Safety Answering Points: Overview and Governance

The emergency services sector is one of 16 critical infrastructure sectors identified by the Department of Homeland Security (DHS) as integral to American national security.[1] While this sector covers multiple areas vital to public safety — law enforcement, fire and rescue services, emergency medical services, emergency management, and public works[2] — these services tend to be geographically-distributed and community-based, showing an overall pattern of local administration in first-response services.[3]

Public Safety Answering Points (or PSAPs) are, for most Americans, the single point of contact for these life-critical requests. PSAPs receive 911 calls and dispatch (or transfer requests to) the appropriate emergency services:[4] operating as twenty-four-hour emergency centers for areas in their jurisdiction. Although PSAPs are one of the most important entities in emergency management, their governance is — by design — also local.[5] While states hold regulatory power over PSAPs,[6] local authorities (such as cities and counties) hold responsibility for designing, implementing, and operating these services.[7] In the context of their importance to national security, this may seem surprising. However, with the diversity of cultures, challenges, and physical circumstances across the United States, local control is thought to be best-positioned for leveraging the strengths of community knowledge in emergency situations.[8]

The federal government's role in PSAPs, then, is limited. The DHS offers initiatives designed to lessen cyber risk for 911 services;[9] [10] and the Federal Communications Commission (FCC) monitors and makes limited rules supporting such services' reliability,[11] although its interstate jurisdiction constrains its power in local telecommunications infrastructure like PSAPs. While some have called for increased action by the FCC in regulating 911 services,[12] these complaints have typically been in response to internet or telephone network outages, rather than the structure or function of PSAPs themselves.

Perhaps the most direct standards across PSAPs nationwide, then, are those offered by professional organizations

like the National Emergency Number Association (NENA). From a security standpoint, NENA offers detailed recommendations, best practices, and checklists for PSAP systems, activities, and audits.[13] [14] [15] NENA also offers comprehensive resources in regard to risk assessment.[16] [17] However, all NENA standards and practices are voluntary[18], so they do not represent a regulatory mandate across the 5,874 PSAPs in the United States.[19]

While calling 911 to access a dispatcher may be a common point of cultural reference for Americans, the reality of PSAP systems is far more complicated. In the age of the Internet of Things (IoT) — in which objects and devices are increasingly internet-connected and engaging in the collection and communication of data[20] — PSAPs are encountering many more technologies and processes for integration with first-response systems.[21] Some examples of such IoT devices include building sensors (like smart smoke detectors, security systems, and industrial controls), personal sensors (for health monitoring), and mobile sensors (such as drones for environmental sampling, or car components for crash detection) — any of which might be integrated with PSAPs for enhanced emergency response times following detection of life-critical circumstances.

With more IoT devices and software originating from both public and private sources, PSAPs increasingly face growing external data — and with it, growing vulnerability to external threats. As the DHS puts it: "*Because our nation is now dependent on properly functioning networks to drive so many life-sustaining activities, IoT security is now a matter of homeland security.*"[22] When it comes to the life-critical functions of PSAPs, the implications of this IoT risk become magnified and ethically significant.

Serverless Computing: A Platform for Life-Critical Functions

Serverless computing has achieved popularity on a timeline similar to IoT ubiquity.[23] While running code on these cloud systems is not literally "serverless" — servers still exist, handled by another party[24] — this type of service *functionally* frees the developer from the logistics of servers, enabling code handoffs that can run without any further infrastructure management.[25] The extreme implication of this is that organizations can transition to a "NoOps" model, in which enterprise IT becomes a thing of the past: developers could be the sole technical hires, deploying code at a faster clip without infrastructure knowledge or barriers.[26] [27] [28] [29] Indeed, serverless architectures are increasingly being adopted by developers because of the convenience that they offer.[30] Conceivably, this model could allow a single developer to manage all aspects of delivering an application.

Serverless computing is sometimes called a Function as a Service (FaaS). Within the FaaS realm, several platforms are currently competing for market share: among them Microsoft's Azure Functions,[31] Google Cloud Functions,[32] and and IBM's Cloud Functions.[33] However, the market leader in serverless computing[34] is currently AWS Lambda (a product of Amazon Web Services).[35] In addition to serving massive customers like Netflix[36] and Expedia,[37] Lambda is also the compute platform that Amazon itself uses for Alexa[38] and its AWS IoT services.[39]

It is beyond the scope of this paper to assess risks in *all* serverless computing platforms. Given Lambda's market share, then, it will be our principal subject for the analysis that follows.

Lambda is already being used in emergency response contexts. Emergency services in the Australian state of Victoria are using AWS services, including Lambda, to manage alerts and responses to natural disasters.[40] Agero, out of Medford, Massachusetts, uses a similar stack (again including Lambda) to cue an emergency response following IoT detection of a severe auto crash.[41] Due to its IoT compatibility, pay-as-you-go-model, and scalability,[42] Lambda may be especially useful for emergency applications like these. When responding to unpredictable events that potentially involve extremely high user loads at irregular intervals, the flexible capacity and lack of fixed costs during downtime are particularly attractive from an emergency operations standpoint.[43]

Lambda is also becoming HIPAA-eligible,[44] a sign that Amazon believes that life-critical services (such as medical applications) can and should be run on the platform. Between this direction in policy and the existing use cases in

emergency scenarios, it becomes clear that Lambda is a platform — and a product security standard — on which people's lives will depend.

Risks to PSAPs

Since Lambda is a major platform on which data may be delivered to/from PSAPs (as described in the previous examples), it follows that Lambda's attack vectors should be examined as part of an overall PSAP risk assessment. As PSAP infrastructure is a known target for terrorism,[45] [46] this becomes especially relevant in a discussion of critical infrastructure.

If life-critical technology running on Lambda is compromised by cyberterrorists, PSAP functions could also be compromised in multiple ways. PSAPs could be fed *false information* from a compromised IoT sensor network[47] running on Lambda, and rescuers could be dispatched to the wrong location during a simultaneous terrorist event elsewhere. Similarly, a sensor network could be completely disabled, thereby veiling an attack in progress. Digital emergency alert systems (running on Lambda, and relaying PSAP data) could also be disabled by a cyberterrorist, thus sending *no information* out to the community, leaving individuals vulnerable in an emergency scenario. Lastly, if PSAP systems *themselves* are running functions on Lambda, they are also directly vulnerable to Lambda's attack vectors.

While such attack vectors would also be possible on another platform (self-hosted or cloud-based), these types of attacks are particularly easy on Lambda for two reasons: The ease of mismanaging a single set of credentials, and the particular policies of Lambda's public code repository. Both of these factors can become vulnerabilities through a combination of lazy security policy and moderate social engineering, as will be described below.

Attack Vectors in Lambda

The AWS default (on account creation) is a single username/password combination that contains all administrative privileges to all services (of which Lambda is one). If a developer does not follow the best practice of creating users with limited permissions[48] — instead maintaining this default root user for all tasks — this single credential, if compromised, has the potential to take the entire Lambda application down. Compromising this credential could be as simple as calling up Craig in accounting and impersonating a need for the AWS password. Since AWS payment and Lambda code controls are locked behind the same credential, it's possible that well-meaning nontechnical employees could have access to the credentials for the root user without understanding the implications therein. In contrast to the days of multiple servers being physically located in somebody's basement, this single sign-on makes Lambda (and AWS as a whole)[49] an attractive target for nefarious remote access. Although this penetration scenario may seem elementary, the pattern of socially engineering a root credential is well-established in the hacking toolkit.[50] [51] [52] Interestingly, one publically-presented working prototype has already demonstrated Lambda exploits based partially on bad AWS identity + access management (IAM) setup.[53]

While the previous scenario is an opportunistic attack on a weak customer target, there is also a risk for more proactive compromises of the serverless ecosystem. As of February 21, 2018,[54] the AWS Serverless Application Repository[55] has been a public, unmoderated resource for sample Lambda code that anyone can run in a single click. Inherent in this is that anyone can engineer a vulnerability into code submitted to the repository — and engineer popularity of this code through manual downloads from different destinations — thereby making the insecure code spread to those who build a dependency on it. (Lambda offers no way to preview the actual source code of uploaded samples within the repository: the user is only offered an external GitHub link[56] to view the source, begging the question of whether a contributor could upload one thing to Lambda, but represent it as another in the supplied external link.) Through following forked code in this system, it becomes easy to reverse engineer who's using that code — and therefore, who has a particular security vulnerability. Although the Serverless Application Repository is undoubtedly a move by Amazon to make its serverless ecosystem more usable, "sticky" and developer-friendly, the

tradeoff with security is nevertheless troubling when viewed through the lens of how easy this code is to access, versus how few security guardrails are mandated by the ecosystem.

Amazon's Stance on Security Practices

AWS has a shared responsibility model[57] for the security of all its cloud services: emphasizing individual customers' responsibility for the security of their own data, code, and access management, while AWS is responsible for infrastructure security. This offers the customer maximum flexibility for configuring and managing their projects, but it also leaves the customer vulnerable should they not take that responsibility seriously (i.e., in a mistaken belief that "the cloud is secure"). While AWS offers security measures to their customers, such as multi-factor authentication (MFA)[58] and resources on best practices,[59] all is optional and up to the customer.

Interestingly, AWS's most recent SOC3 specifically disclaims cybersecurity risk management in its scope, and notes "human error" and "circumvention of controls" as inherent limitations of the SOC3 assessment.[60] AWS management echoes this in an appendix to the SOC3, noting that "ineffective controls at a vendor or business partner" are inherently beyond the scope of AWS's security controls.[61] At a recent AWS Re:Invent presentation, a customer also echoed this division of responsibilities, noting that "good AWS IAM [identity and access management] account setup […] will be key to showing good governance" once an AWS customer moves into SOC2 compliance[62] — although, once again, this responsibility falls on the customer.

Who is Responsible?

Should a breach in a Lambda application affect a PSAP, as imagined in our scenario, who would be responsible? The federal government does not regulate the details of PSAPs or of Lambda; state regulations would likely not be granular enough to spell out technical security practices; NENA guidelines are strictly voluntary; and Amazon specifically disclaims responsibility for everything but infrastructure. Ultimately, it is the local PSAP authorities who are responsible for making all decisions about their own security and data policies — including the decision to trust a developer offering a useful integration. Similarly, it is the developer's responsibility to secure their application.

But from a practical perspective — with nearly six thousand independent PSAPs, and untold numbers of developers working on technology that could integrate with emergency response — expecting everyone to execute flawlessly on their responsibilities may be unrealistic.

What Needs to Change?

Although we may have a clear answer for *legal* accountability in the event of a breach, the answer on *ethical* accountability may be broader than this.

In supporting life-critical applications — indeed, in *seeking* them through HIPAA compliance — AWS Lambda has become a steward (no matter how reluctantly) of people's lives. Yet, rather than building policies and principles that reflect the gravity of this reality, Amazon continues its libertarian attitude toward its customer community: offering security resources, but not taking a strong stance on them. In the context of a peer group doing otherwise — Facebook building features to detect and counteract self-harm,[63] Twitter writing algorithms to counteract abusive users,[64] Google creating proactive responses to searches indicating at-risk status[65] — this is a disappointing response to an important burden.

Amazon has the opportunity to create a culture of security in its Lambda user community. Much like how it incentivizes its own employees to seek out training and expertise (via phone tool icons[66]), Amazon could incentivize its user community to become security experts through more visible and socially-enforced user education: promoting the existing AWS certification program (which includes a security component)[67] as a less-optional industry standard, and rewarding developers who complete it with discounts on AWS services. Amazon could similarly incentivize customer use of multi-factor authentication by offering discounts for those who use it, or even

requiring that applications involving a life-critical component use MFA as a non-negotiable security measure. Amazon could evaluate code before adding it to the Serverless Application Repository — much like how Apple reviews all apps that are submitted to its App Store.[68] And Amazon could also allow the user to preview repository code directly, resolving the uncertainty of whether such code could be misrepresented by its originator. However, as it currently stands, Amazon's hands-off attitude on these issues sets a clear — yet indifferent — tone at the top.[69]

Although Amazon is not known for a strong stance on corporate social responsibility — only hiring a director for this role in 2015,[70] twenty-one years into its existence — this history does not stand in the way of its potential future of proactively-responsible stewardship. As a market leader with Lambda, Amazon has the opportunity to set policy at the same time as they mitigate risks in their serverless computing ecosystem. The business value of such mitigation is directly expressed in their 2018 10-K filing:

> As a result of our services being web-based and the fact that we process, store, and transmit large amounts of data, including personal information, for our customers, failure to prevent or mitigate data loss or other security breaches, […] could expose us or our customers to a risk of loss or misuse of such information, adversely affect our operating results, result in litigation or potential liability for us, and otherwise harm our business.[71]

A voluntary change in security tone and policy could be both a marketing tool, and a hedge against the risk (reputational and otherwise) inherent in being the site of a crisis, should a life-critical Lambda breach happen. Indeed, user security education ultimately aligns with Amazon's business, with citizens' interests, and with PSAPs' security needs. For a company touting "customer obsession"[72] as a core principle, this seems like an ethically- and financially-sound investment.

A Role for Government

While it can be argued that enhanced regulation of PSAPs could lead to stronger security standards and greater compliance, the original intention of PSAPs' independent governance holds some weight. Allowing local knowledge, priorities, and culture to inform emergency response gives individual PSAPs the freedom to allocate their resources in response to local trends; collaborate with individuals and community organizations which may assist in the overarching public safety mission; and nurture public/private partnerships with owners of infrastructure that holds importance to the community's overall wellbeing. Applying a set of standard rules, particularly in response to new technology, risks quashing progress and efforts of local importance. PSAPs may be the best judges of risk/reward equations in their jurisdictions, due to their authority on the area.

However, attainably-designed mandates may offer a realistic improvement in security, without compromising innovation significantly. States could require that any third-party software or device linked to PSAPs be developed by someone with the appropriate evidence of security-specific study: Perhaps, in this way, the AWS credential could gain some teeth (especially if Amazon partnered with government stakeholders in the credential's design). To use the metaphor of a pilot's license or a lawyer's bar admission: government has determined in the past that positions with the potential for harming others through their practice should be regulated by a credentialing process in which mastery is demonstrated. When it comes to platforms, software, and data that determines the course of human lives, this seems all too appropriate.

Technology — and Policy — Designed for Humans

AWS Lambda is undoubtedly designed with ease of use at the forefront. From streamlining developers' responsibilities, to managing everything from a single set of credentials, to offering crowdsourced off-the-shelf code: Lambda's ecosystem reflects the tremendous importance Amazon places on usability. However, it is exactly that degree of usability which catalyzes the vulnerabilities discussed above.

When a product such as Lambda poses such powerful possibilities in the public sphere, at what point is developers' ease-of-use a liability for the people? Within Lambda's design and defaults, it is easier to ignore security than it is to master it. And although this "frictionlessness" is attractive to software developers, the overall lack of security culture and incentives in Lambda creates an environment in which the actions (or inactions) of an ignorant or inexperienced developer may cause grave public consequences.

In this author's opinion, the key takeaway for future Lambda development is the idea of proportionality: an idea described by Sons, Jackson and Russell[73] as "*tailoring security strategies to the magnitude of the risks*." If Lambda (and its Serverless Application Repository) were conceived as products for conventional business applications, the current evidence of life-critical use should provoke reflection on the human cost of disproportionate usability and insufficient security incentives. Although PSAPs are one downstream example of these implications, they are not the only one. In the context of Amazon's love for human-centered design, perhaps security policy *itself* can be factored into human-centeredness — when the end customer is all of us.

---

[1] "Critical Infrastructure Sectors." The US Department of Homeland Security. 11 July 2017. Accessed 5 March 2018. <https://www.dhs.gov/critical-infrastructure-sectors>.

[2] "Emergency Services Sector." The US Department of Homeland Security. 26 January 2018. Accessed 5 March 2018. <https://www.dhs.gov/emergency-services-sector>.

[3] "911 Master PSAP Registry." Federal Communications Commission. 1 March 2018. Accessed 5 March 2018. <https://www.fcc.gov/general/9-1-1-master-psap-registry>.

[4] "E9-1-1 Public Safety Answering Points." Connecticut Department of Emergency Services and Public Protection. 1 August 2016. Accessed 5 March 2018. <http://www.ct.gov/despp/cwp/view.asp?a=4437&Q=515090&desppNAV_GID=2127&desppNav=&pp=3>.

[5] "History of 911." Industry Council for Emergency Response Technologies. n.d. Accessed 5 March 2018. <https://www.theindustrycouncil.org/publications/iCERT-9EF_Historyof911_WebVersion.pdf>.

[6] "2017 Key Enacted 911 Legislation." National Conference of State Legislatures. 22 January 2018. Accessed 5 March 2018. <http://www.ncsl.org/research/telecommunications-and-information-technology/2017-key-enacted-911-legislation.aspx>.

[7] "History of 911."

[8] "History of 911."

[9] "Emergency Services Sector Cybersecurity Initiative." US Department of Homeland Security. 20 June 2017. Accessed 5 March 2018. <https://www.dhs.gov/emergency-services-sector-cybersecurity-initiative>.

[10] "Cyber Risks to Next Generation 911." US Department of Homeland Security. n.d. Accessed 5 March 2018. <https://www.911.gov/pdf/OEC_Fact_Sheet_Cyber_Risks_NG911.pdf>.

[11] "Policy Statement and Notice of Proposed Rulemaking In the Matters of 911 Governance and Accountability Improving 911 Reliability." Federal Communications Commission. 21 November 2014. Accessed 5 March 2018. <https://apps.fcc.gov/edocs_public/attachmatch/FCC-14-186A1_Rcd.pdf>.

[12] Stephens, Joe, and Flaherty, Mary Pat. "Federal lawmakers call for stemming failures of 911 services." *The Washington Post.* 4 December 2012. Accessed 5 March 2018. <https://www.washingtonpost.com/local/federal-lawmakers-call-for-stemming-failures-of-911-services/2012/12/04/9022f8dc-3e2d-11e2-ae43-cf491b837f7b_story.html?utm_term=.5809bf7eb6a4>.

[13] "NENA Next Generation 9-1-1 Security (NG-SEC) Information Document." National Emergency Number Association (NENA). 8 December 2016. Accessed 5 March 2018. <https://c.ymcdn.com/sites/www.nena.org/resource/resmgr/standards/NENA-INF-015_NGSEC_INF_20161.pdf>.

[14] "NENA Security for Next-Generation 9-1-1 Standard (NG-SEC)." National Emergency Number Association (NENA). 6 February 2010. Accessed 5 March 2018. <https://c.ymcdn.com/sites/www.nena.org/resource/resmgr/Standards/NENA_75-001.1_NG-Security_20.pdf>.

[15] "Next Generation 9-1-1 Security (NG-SEC) Audit Checklist." National Emergency Number Association (NENA). 14 December 2011. <https://c.ymcdn.com/sites/www.nena.org/resource/resmgr/Standards/NENA_75-502.1_NG-

SEC_Audit_C.pdf>.

[16] "NENA Resource, Hazard and Vulnerability Analysis Information Document." National Emergency Number Association (NENA). 10 September 2016. Accessed 5 March 2018. <http://c.ymcdn.com/sites/www.nena.org/resource/resmgr/standards/NENA-INF-019.2-2016_Hazard_A.pdf>.

[17] "NENA Communications Center/PSAP Disaster and Contingency Plans Model Recommendation." National Emergency Number Association (NENA). 12 November 2015. Accessed 5 March 2018. <http://c.ymcdn.com/sites/www.nena.org/resource/resmgr/Standards/NENA-INF-017.2.2015_Disaster.pdf>.

[18] "Next Generation 911 (NG911) Standards Identification and Review." 911.Gov. March 2016. Accessed 5 March 2018. <https://www.911.gov/pdf/National_911_Program_NG911_Standards_Identification_Analysis_2016.pdf>.

[19] "Emergency Services Sector Profile." US Department of Homeland Security. November 2017. Accessed 5 March 2018. <https://www.dhs.gov/sites/default/files/publications/18_0126_NPPD_emergency-services-sector-profile-v2.pdf>.

[20] Burgess, Matt. "What is the Internet of Things? WIRED explains." *Wired.* 16 February 2018. Accessed 5 March 2018. <http://www.wired.co.uk/article/internet-of-things-what-is-explained-iot>.

[21] "Public Safety Digital Transformation: The Internet of Things (IoT) and Emergency Services." European Emergency Number Association. 3 March 2016. Accessed 5 March 2018. <http://www.eena.org/download.asp?item_id=170>.

[22] "Strategic Principles for Securing the Internet of Things (IoT)." US Department of Homeland Security. 15 November 2016. Accessed 5 March 2018. <https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf>.

[23] Boyd, Mark. "What Serverless and the Internet of Things Can Learn from Each Other." *The New Stack*. 4 May 2017. Accessed 5 March 2018. <https://thenewstack.io/iot-serverless-can-learn/>.

[24] Butler, Brandon. "Serverless explainer: The next generation of cloud infrastructure." *Network World*. 3 April 2017. Accessed 5 March 2018. <https://www.networkworld.com/article/3187093/cloud-computing/serverless-explainer-the-next-generation-of-cloud-infrastructure.html>.

[25] "Serverless Computing and Applications." Amazon Web Services, Inc. n.d. Accessed 5 March 2018. <https://aws.amazon.com/serverless/>.

[26] Pariseau, Beth. "Serverless computing supporters ponder NoOps." *TechTarget*. 31 May 2016. Accessed 5 March 2018. <http://searchitoperations.techtarget.com/news/450297503/Serverless-computing-supporters-ponder-NoOps>.

[27] Boyd, Mark. "The Road to NoOps: Serverless Computing is Quickly Gaining Momentum." *The New Stack*. 18 May 2016. Accessed 5 March 2018. <https://thenewstack.io/serverless-computing-growing-quickly/>.

[28] Boeckman, Matthew. "Ops, DevOps, NoOps and AWS Lambda." 24 April 2015. Accessed 5 March 2018. <https://www.slideshare.net/MatthewBoeckman/ops-devops-noops-and-aws-lambda>.

[29] Duff, Steven. "When should I use AWS Lambda versus Amazon EC2?" 30 June 2016. Accessed 5 March 2018. <https://cloudranger.com/aws-lambda-versus-amazon-ec2/>.

[30] Asay, Matt. "Convenience, not cost, is driving serverless adoption among developers." *TechRepublic*. 8 January 2018. Accessed 5 March 2018. <https://www.techrepublic.com/article/convenience-not-cost-is-driving-serverless-adoption-among-developers/>.

[31] "Azure Functions." Microsoft. n.d. Accessed 5 March 2018. <https://azure.microsoft.com/en-us/services/functions/>.

[32] "Cloud Functions." Google. n.d. Accessed 5 March 2018. <https://cloud.google.com/functions/>.

[33] "IBM Cloud Functions." IBM. n.d. Accessed 5 March 2018. <https://www.ibm.com/cloud/functions>.

[34] Hecht, Lawrence. "AWS Lambda Still Towers Over the Competition, but for How Much Longer?" The New Stack. 9 December 2017. Accessed 5 March 2018. <https://thenewstack.io/aws-lambda-still-towers-competition-much-longer/>.

[35] "AWS Lambda." Amazon Web Services. n.d. Accessed 5 March 2018. <https://aws.amazon.com/lambda/>.

[36] "Netflix & AWS Lambda Case Study." Amazon Web Services. n.d. Accessed 5 March 2018. <https://aws.amazon.com/solutions/case-studies/netflix-and-aws-lambda/>.

[37] Asay, Matt. "Serverless architecture is the future, but we're not getting rid of containers just yet." *TechRepublic.* 11 January

2018. Accessed 5 March 2018. <https://www.techrepublic.com/article/serverless-architecture-is-the-future-but-were-not-getting-rid-of-containers-just-yet/>.

[38] Butler, Brandon. "What is Amazon cloud's Lambda and why is it a big deal?" NetworkWorld. n.d. Accessed 5 March 2018. <https://www.networkworld.com/article/3053111/cloud-computing/what-is-amazon-cloud-s-lambda-and-why-is-it-a-big-deal.html>.

[39] Lardinois, Frederic. "AWS Greengrass brings Lambda to IoT devices." *TechCrunch.* 30 November 2016. Accessed 5 March 2018. <https://techcrunch.com/2016/11/30/aws-greengrass-brings-lambda-to-iot-devices/>.

[40] Foye, Brendon. "Base2Services deploys serverless computing on AWS for Victorian emergency services app." *CRN Australia*. 9 March 2017. Accessed 5 March 2018. <https://www.crn.com.au/news/base2services-helps-emv-go-serverless-on-aws-for-victorian-emergency-services-453857>.

[41] "Agero Works to Improve Driver Safety Using Amazon Web Services." Agero, Inc. 6 December 2016. Accessed 5 March 2018. <https://www.agero.com/agero-works-improve-driver-safety-using-amazon-web-services>.

[42] "What Is AWS Lambda?" Amazon Web Services, Inc. n.d. Accessed 5 March 2018. <https://docs.aws.amazon.com/lambda/latest/dg/welcome.html>.

[43] Foye, Brendon.

[44] Hatt, Nick. "AWS Lambda has been HIPAA Eligible for a Month, and it's Awesome." Redox, Inc. 28 November 2017. Accessed 5 March 2018. <https://www.redoxengine.com/engineering/aws-lambda-hipaa-eligible>.

[45] Proffitt, Chris. "DPS: Cyberattack on city's communication system." *The Indy Channel*. 20 January 2015. Accessed 5 March 2018. <https://www.theindychannel.com/news/local-news/dps-cyberattack-on-citys-communication-system>.

[46] Guri, Mordechai, Mirsky, Yisroel, and Elovici, Yuval. "9-1-1 DDoS: Threat, Analysis and Mitigation." Ben-Gurion University of the Negev. d.d. Accessed 5 March 2018.<https://arxiv.org/pdf/1609.02353.pdf>.

[47] Stone, Adam. "Emergency Agencies Prepare for Cyberbreaches to 911 Systems." *Government Technology*. 21 January 2014. Accessed 5 March 2018. <http://www.govtech.com/state/Emergency-Agencies-Cyberbreaches-911.html>.

[48] "IAM Best Practices." Amazon Web Services, Inc. n.d. Accessed 5 March 2018. <https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html>.

[49] Venezia, Paul. "Murder in the Amazon cloud." *Info World.* 23 June 2014. Accessed 5 March 2018. <https://www.infoworld.com/article/2608076/data-center/murder-in-the-amazon-cloud.html>.

[50] Bright, Peter. "Anonymous speaks: the inside story of the HBGary hack." *ArsTechnica.* 15 February 2011. Accessed 5 March 2018. <https://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/3/>.

[51] Criddle, Linda. "What is Social Engineering?" Webroot. n.d. Accessed 5 March 2018. <https://www.webroot.com/us/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering>

[52] "What is social engineering?" Symantec Corporation. n.d. Accessed 5 March 2018. <https://us.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html>.

[53] Jones, Rich. "Gone in 60 Milliseconds: Intrusion and Exfiltration in Server-less Architectures." 28 December 2016. Accessed 5 March 2018. <https://media.ccc.de/v/33c3-7865-gone_in_60_milliseconds#t=846>.

[54] Frank, Blair Hanley. "AWS' Serverless Application Repository compounds its early advantage." *VentureBeat.* 21 February 2018. Accessed 5 March 2018. <https://venturebeat.com/2018/02/21/aws-serverless-application-repository-compounds-its-early-advantage/>.

[55] "AWS Serverless Application Repository." Amazon Web Services, Inc. n.d. Accessed 5 March 2018. <https://aws.amazon.com/serverless/serverlessrepo/>.

[56] Screenshot dated March 15th, 2018, showing a GitHub link as the sole means of viewing source code: <https://drive.google.com/file/d/1jTOw6s2nNfdIZ7WcLptLQpB8xSoxpQfL/view?usp=sharing>

[57] "Shared Responsibility Model." Amazon Web Services, Inc. n.d. Accessed 5 March 2018. <https://aws.amazon.com/compliance/shared-responsibility-model/>.

[58] "Multi-Factor Authentication." Amazon Web Services, Inc. n.d. Accessed 5 March 2018. <https://aws.amazon.com/iam/details/mfa/>.

[59] "IAM Best Practices."

[60] "System and Organization Controls 3 (SOC 3) Report." Amazon Web Services, Inc. 26 October 2017. Accessed 5 March 2018. <https://d1.awsstatic.com/whitepapers/compliance/AWS_SOC3.pdf>.

[61] "System and Organization Controls 3 (SOC 3) Report."

[62] Hagopian, Matt. "Effective Emergency Response in AWS: LiveSafe." 27 November 2017. Accessed 5 March 2018. <https://www.slideshare.net/AmazonWebServices/wps204effective-emergency-response-in-awspdf>.

[63] Brown, Jennings. "Facebook Expands Self-Harm Prevention Program That Monitors Users' 'Thoughts of Suicide.'" *Gizmodo*. 27 November 2017. Accessed 5 March 2018. <https://gizmodo.com/facebook-expands-suicide-prevention-program-that-monito-1820771685>.

[64] Ingram, Mathew. "Twitter Is Now Trying to Detect and Curb Abuse in Real Time." *Fortune.* 1 March 2017. Accessed 5 March 2018. <http://fortune.com/2017/03/01/twitter-abuse-real-time/>.

[65] Widner, Kasumi, and Busselle, Chris. "UPDATE: Helping Human Trafficking and Modern Day Slavery Victims Around the World." 12 January 2015. Accessed 5 March 2018. <https://publicpolicy.googleblog.com/2015/01/update-helping-human-trafficking-and.html>.

[66] Flair on an employee's internal profile that functions like merit badges, received for completing certain tasks, education, or accomplishments.

[67] "AWS Certification." Amazon Web Services, Inc. n.d. Accessed 5 March 2018. <https://aws.amazon.com/certification/>.

[68] "App Review." Apple, Inc. n.d. Accessed 5 March 2018. <https://developer.apple.com/app-store/review/>.

[69] "Tone at the Top and Third Party Risk." Ponemon Institute and Shared Assessments. May 2016.

[70] Banjo, Shelly. "After public outrage over worker treatment, Amazon's hiring a director of social responsibility." *Quartz*. 9 September 2015. Accessed 5 March 2018. <https://qz.com/498320/after-public-outrage-over-worker-treatment-amazons-hiring-a-director-of-social-responsibility/>.

[71] "Form 10-K 2018." Amazon.com, Inc. 1 February 2018. Accessed 5 March 2018. <https://www.sec.gov/Archives/edgar/data/1018724/000101872418000005/0001018724-18-000005-index.htm>.

[72] "Leadership Principles." Amazon.com, Inc. n.d. Accessed 5 March 2018. <https://www.amazon.jobs/principles>.

[73] Sons, Susan, Jackson, Craig, and Russell, Scott. "Chapter 7: Proportionality." O'Reilly. October 2017. Accessed 5 March 2018. <https://www.safaribooksonline.com/library/view/security-from-first/9781491996911/ch07.html>.