How Assembla Approaches Security

by Jacek Materna, CTO

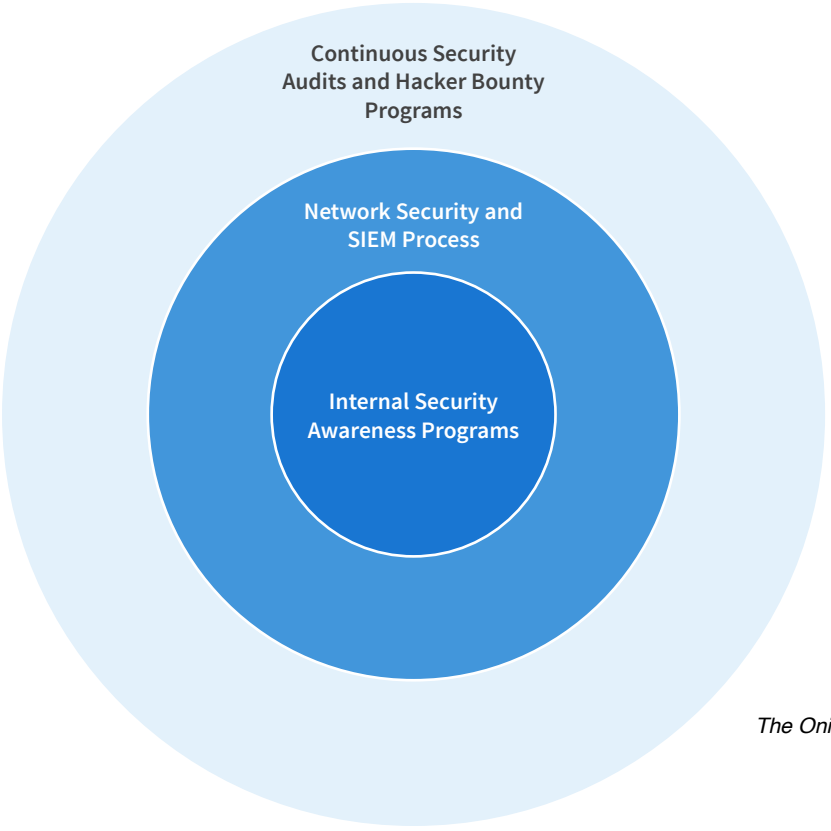
ASSEMBLA

Setting our customers up for success is always a top priority for us at Assembla, from the quality of our product to how we deliver and support it. For our DevOps team, we're obsessed with global uptime, application performance and security. As the CTO I can say that we work tirelessly to keep all services running smoothly and securely.

Having spent the better part of the last 15 years in network security building, hacking and selling network security software across various verticals, I'm passionate about security and take it very seriously. I understand and have seen first hand the implications of not positioning security at the forefront of your business. As such Assembla keeps Security at the boardroom level.

At Assembla, how we handle network threats today and in the future is a top priority for us. In fact, network security is a strategic initiative at Assembla because it's closely tied with the availability of our services and this goes back to ensuring our customers are set up for success.

We approach security at Assembla as "Defense in Depth" which we like to call "The Onion."

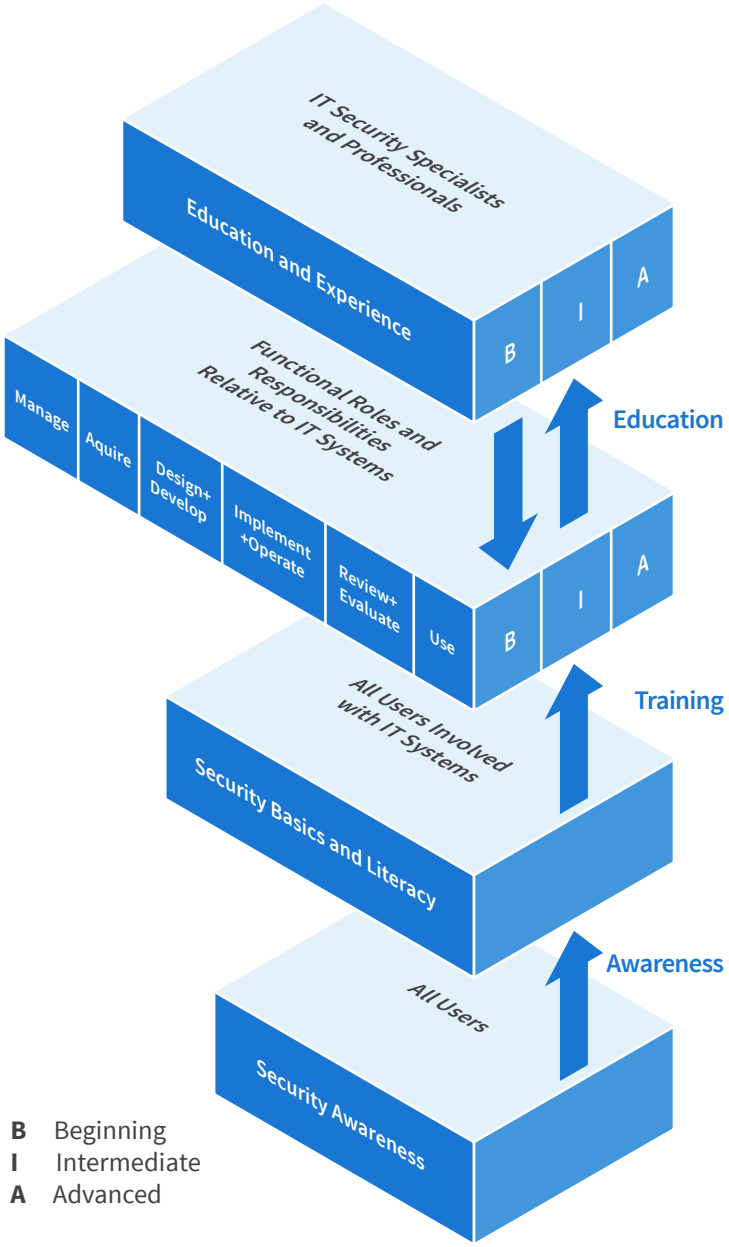


The Onion

Security Awareness Program

At the core of our strategy lies our Security Program that was designed specifically for all Assembla staff and employees. We know that the majority of security breaches occur due to leaks in internal processes and it's not uncommon for employees not to be unaware that how they go about their everyday processes and procedures could impact customer data and the integrity of our internal systems. This is the responsibility of the CTO, not the employees, to ensure the entire organization is educated and fully trained on security best practices and requirements and that is what our Security Awareness Program is built upon.

Knowledge of threats goes a long way in educating everyone and reinforcing good behavior across the board.



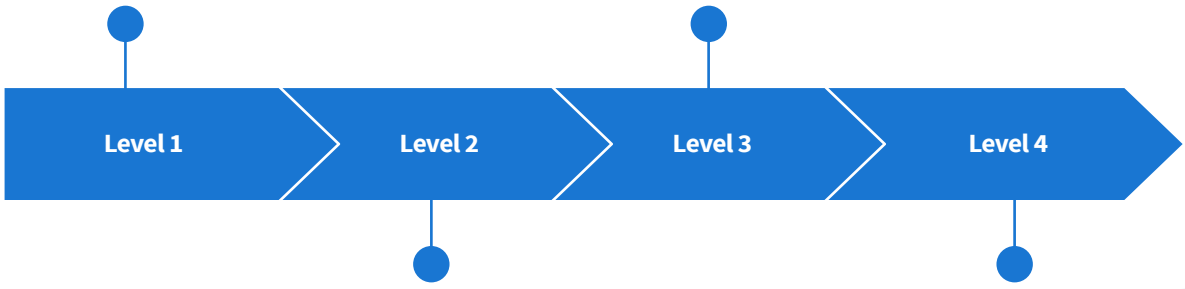
Network Security and Security Incident and Event Management (SIEM)

Assembla runs in a hybrid cloud environment with high performance IO applications running in our Equinox DCs and AWS data centers, to ensure our customers' code repositories are always up and running and are fast. We've invested heavily into hardware, software based perimeter defense, including post breach monitoring and mitigation systems.

We have strong processes set up internally to compartmentalize access to data and key systems. Assembla staff touch and interact with multiple systems that have customer data at rest. We use a variety of tools that reference or contain data about customers and their data which is why we follow strict access control restrictions. We make sure tools only have the bare minimum needed to get their job done and security audits are performed regularly.

Since customer data in a multi-tenant environment is shared by definition, strict controls and policies must exist to compartmentalize access to data in transit and at rest. To monitor, maintain and coordinate these processes, we run a four step Security Incident Response Killchain which is coordinated by our Security Operations Center (SOC).

The SOC is constantly monitoring the perimeter, application usage for nefarious activity using our SIEM system. We invest a lot of money and resources monthly ensuring we have a very solid defense for our customers.



Continuous Audits and Hacker Bounty

Assembla uses HackerOne, a leading premier vulnerability coordination platform.
The basics of HackerOne are simple. Assembla creates our own security program page with instructions for hackers:

- what targets are in scope
- what types of findings are eligible and not
- what rewards we'll be paying
- what behaviors are acceptable
- what the ideal vulnerability report should look like

We then set bug bounty awards by technical classification of the bug and severity of its possible impact. We set a minimum of $100. The average is around $500 but it could be more. To get attention from the world's best hackers, you want to pay more than the platform average.

Who are the hackers?

Your hackers, also called security researchers or finders, are selected from the top tier of HackerOne. You can invite your own hackers, or HackerOne can customize your invitations for your specific needs. Your program starts private but can be made public. As bugs come in we review the reports for validity, using the report's proof of concept and the hacker's reputation on HackerOne. If valid, we prioritize the fix to the vulnerability in our backlog.

Why a bounty program?

I've been in security long enough to know that bounty programs are a critical piece to ensure a quality security program. In the past, they were secret communities. Now we have a range of options that bring hackers and organizations together, imagine that. Security is hard because it is unfalsifiable. I can't say that I've found all the bugs in any given program so I try to stack the odds in my favor by layering systems that surface bugs: design reviews, code reviews, type systems, program analysis, external security audits, blackbox scanning, etc. Bounty programs sit at the end of this process which means every bug found is one that slipped past everything thrown at it. Bounty programs are a good fit with agile development practices. In the old days you planned 6 months of software development, you hit your deadlines, it went to QA, then it shipped.

Today everyone does agile because it ships faster; continuous and legacy QA teams are near extinction. Bounty programs fit this environment great because fixes can be pushed quickly and act as informal QA. However, a bounty program does not replace anything you are or should be doing security-wise, it just augments it; it's the icing on the software development lifecycle cake. A bounty program does not replace consultants, they are different tools to achieve different things. If you want to discover a whole lot of security bugs however, bounty programs are a good bet.

HackerOne is the best offer on the market to today in my opinion. It's a SaaS take on a world that has existed in secrecy which is exciting in its own regards because it gives anyone access to this deep talent pool to have more secure software on the web. HackerOne ensures our production services are clean and stay clean as we push more features to customers.

Assembla Security Incident Handling

All Security Incidents must be reported in accordance with this Section. Diagram A provides an overview of the internal Privacy Incident reporting process at Assembla.

Tier 1: Assembla Personnel
Upon discovery or detection of a potential Incident, Assembla personnel are responsible for immediately reporting the incident to the Support Desk via email support@assembla.com. If the Support Desk is unavailable, Assembla personnel may report the incident directly to the Security Entity or Privacy Officer.

Tier 2: Assembla Support Desk
The Support Desk will evaluate the incident with assistance from the Privacy Officer for the area which the incident occurred. The Support Desk will make a Preliminary Written Report to the Security Entity, if available. If the Security Entity is not available to handle reporting for the incident, the report may be provided to the Assembla SOC.

Tier 3: Privacy Officer/Security Entity Team
The Privacy Officer must immediately consult and evaluate the factual basis of the incident. The Privacy Officer and the Security Entity must develop the factual basis for an accurate and complete report.

The circumstances surrounding the incident will determine whether the Privacy Officer or the Security Entity opens, prepares, and submits the Privacy Incident report of the incident in the internal Incident Handling System.

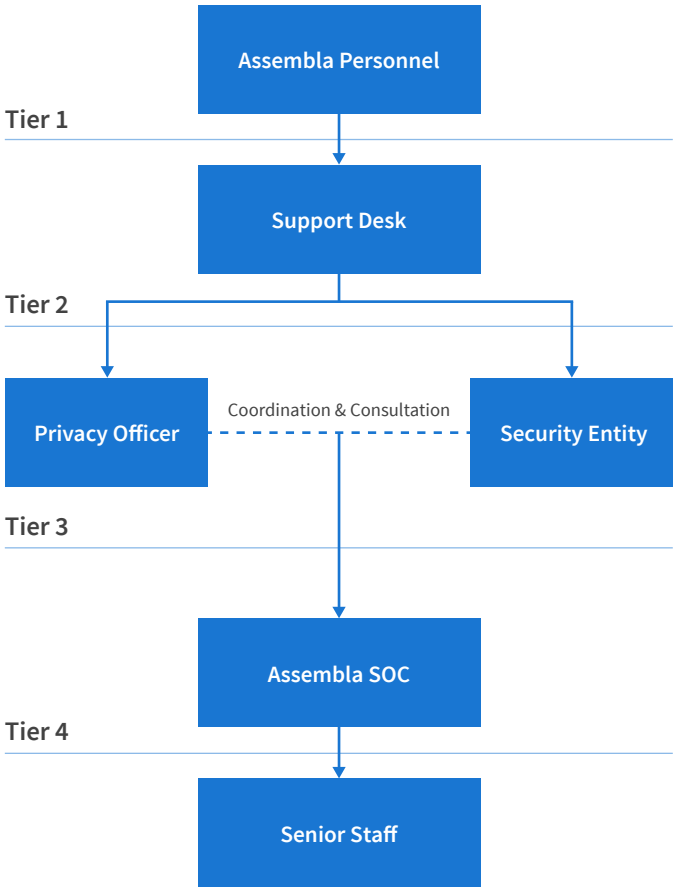


Diagram A

Support Desk
support@assembla.com

Privacy Officer
privacy@assembla.com

Security Entity
security@assembla.com

Assembla SOC
operations@assembla.com

If the Security Entity is unavailable, the Assembla SOC will prepare and submit the report to meet the strict Privacy Incident reporting time requirements.

Tier 4: Assembla SOC
The Assembla SOC will review the Privacy Incident Report for factual sufficiency and transmit the report to internal senior staff within one hour of receiving the Privacy Incident Report from Tier 3.

Supplementation of the Privacy Incident Report

After Assembla SOC has reported the Privacy Incident to internal senior staff, the Privacy Officer must supplement the Privacy Incident Report, as appropriate, with any further factual information that will facilitate the handling of the Privacy Incident. Supplemental information can include factual information solicited, or other information related to the escalation, investigation, notification, mitigation, or incident closure stages of incident handling.

Security Certifications

Assembla is committed to infrastructure compliance and security. Our data centers and infrastructure partners meet strict standards for data and services as follow:

Certifications / Attestations	Laws, Regulations, and Privacy	Alignments / Frameworks
C5 [Germany]	CISPE	CIS
Cyber Essentials Plus [UK]	EU Model Clauses	CJIS
DoD SRG	FERPA	CSA
FedRAMP	GLBA	ENS [Spain]
FIPS	HIPAA	EU-US Privacy Shield
IRAP [Australia]	HITECH	FFIEC
ISO 9001	IRS 1075	FISC
ISO 27001	ITAR	FISMA
ISO 27017	My Number Act [Japan]	G-Cloud [UK]
ISO 27018	U.K. DPA - 1988	GxP (FDA CFR 21 Part 11)
MTCS [Singapore]	VPAT / Section 508	ICREA
PCI DSS Level 1	EU Data Protection Directive	IT Grundschutz [Germany]
SEC Rule 17-a-4(f)	Privacy Act [Australia]	MITA 3.0
SOC 1	Privacy Act [New Zealand]	MPAA
SOC 2	PDPA - 2010 [Malaysia]	NIST
SOC 3	PDPA - 2012 [Singapore]	PHR
	PIPEDA [Canada]	Uptime Institute Tiers
	Spanish DPA Authorization	UK Cloud Security Principles

In addition Assembla is committed to certification of our organization overlaid onto these providers.

As of this writing Assembla has acquired the following corporate certifications:

EU-US
PRIVACY SHIELD

Privacy Shield

The EU-U.S. Privacy Shield Framework was designed by the U.S. Department of Commerce and the European Commission and Swiss Administration to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union to the United States in support of transatlantic commerce.

SOC II Type 1

Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy. These reports are intended to meet the needs of a broad range of users that need detailed information and assurance about the controls at a service organization relevant to security, availability, and processing integrity of the systems the service organization uses to process users' data and the confidentiality and privacy of the information processed by these systems. These reports can play an important role in:

- Oversight of the organization
- Vendor management programs
- Internal corporate governance and risk management processes
- Regulatory oversight

Assembla is committed to certified Security and Availability principles.

HIPAA (1H 2018)

Assembla provides you with a detailed testing approach, based on the OCR protocol for the HIPAA security and privacy safeguards as well as the HITECH breach notification requirements and an exclusive team with extensive technology risk and healthcare audit experience.

GDPR (1H 2018)

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU. The GDPR aims primarily to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. When the GDPR takes effect, it will replace the data protection directive (officially Directive 95/46/EC) of 1995.

PCI Level 3

Assembla is Level 3 PCI certified and partners with Level 1 provider Chargify to process financial transactions.

www.assembla.com