Improving the world’s cyber resilience, at scale

Implementing baseline security by default

Freddy Dezeure, Prof. Lokke Moerel, and Dr. George Webster*

The challenge

We recently published the article “*Digital Sovereignty Is Impossible Without Big Tech*,”[1] calling upon Microsoft, Amazon, and Google to “**improve cybersecurity worldwide by implementing *baseline security by default***” as well as upon EU and U.S. governments to support this endeavor. In our earlier paper we focused on the necessity to increase societies’ cyber resilience in the light of the increasing digital dependencies and cyber risks, the realities of hybrid war, and the changing geopolitical environment. That paper generated a positive response and valuable feedback. To further the discussion, this paper elaborates on ***baseline security by default*** and provides recommendations on how it can be achieved.

It is commonplace for organizations to be dependent on cloud infrastructure and services from Microsoft, Amazon, and Google. In turn, our societies are reliant on their effective operations and ramifications are felt across our economies, our health, our national security, and frankly our well-being. The cloud offers advantages in terms of availability and scalability, but the technical complexity of configuring and securing it, is beyond the capacity of most organizations, even mature ones. Financial institutions reportedly are spending millions per year per enterprise to implement baseline security and the result is still lacking in consistency.

Sane security options must be enabled and maintained on a continual basis or are only available as a separate service, if customers are even aware of them at all. To illustrate, organizations require a secure back-up of their data to recover from a ransomware attack, but many wrongly assume that their data is backed-up by their cloud provider by default.

In our first paper, we concluded that the system whereby we rely on customers to implement secure configurations, controls, and policies results in our infrastructure being **ill-configured and insecure by default**. Few have the means to overcome this challenge; most don’t. This has led to a thriving economy of cyber criminals hacking our infrastructure and an equally thriving economy of vendors, integrators, and consultants promising to protect it.

Our system is broken. We called upon Big Tech to unburden their user organizations of the many duplicative efforts of verifying, implementing, and maintaining recommended security baselines, and thereby improve the world’s cyber resilience, at scale. We acknowledge this is a complex problem and in turn call on governments to enable these companies to do so for the benefits of society.

The opportunity

Most experts consider that better baseline security would dramatically reduce the risk. Microsoft claims that the implementation of five baseline controls could protect against 99% of the attacks.[2] There is no question that Big Tech providers have the capacity, the skills, and the resources to configure, deploy, and maintain secure configurations, policies, and controls *by default* **across their customers’ infrastructure**. This would go beyond what is traditionally

- Freddy Dezeure is an independent strategic advisor and the former head of the EU Institutions’ Computer Emergency Response Team (CERT-EU); Lokke Moerel is a professor of Global ICT Law at Tilburg University, a member of the Dutch Cyber Security Council, and the chair of the Netherlands Atlantic Association; George Webster is the CEO of a stealth startup and the former Chief Security Architect at HSBC.

[1] https://www.atlcom.nl/artikel-atlantisch-perspectief/digital-sovereignty-is-impossible-without-big-tech-a-call-to-action/. The current paper partly draws from this earlier publication.

[2] https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023.

understood as product security because it extends to implementing and maintaining controls in the user environment.

The websites of Microsoft, Amazon, and Google provide extensive guidance for their users about how to implement secure cloud configurations. Similar user guidance is also provided by the national cybersecurity centers of many countries. Although this guidance is disseminated with the best intentions, it remains a huge challenge for users to keep track of and deploy this myriad of scattered and regularly changing guidance. The teams required to keep pace also require specialized skillsets and are rare in the marketplace.

A case in point is the *Secure Configuration Baselines*,[3] published by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) for implementing Microsoft 365 and Google Workspace by the U.S. executive branch to:

> properly address cybersecurity and visibility gaps within cloud-based business applications that have hampered our collective ability to adequately understand and manage cyber risk across the Federal and IT enterprise.

Each of these baselines contains 100+ pages of instructions for the U.S. agencies to configure the options to comply with their statutory security obligations. This begs the obvious question: if such settings must be implemented by all agencies to ensure baseline security and compliance with law, why not require vendors to implement these by default in the first place, reducing duplication of efforts and guaranteeing the outcome?

Legal environment

The concept of “security by default” is not a new concept. Regulators around the world have caught up on the lack of built-in security offered by providers of digital products and services. Both in the U.S. and the EU, regulators have issued cybersecurity strategies indicating that a shift in responsibilities is required, whereby the providers of digital products and services will become liable for providing security by default rather than pass the burden to their users. In the words of the national cybersecurity strategy announced by the U.S. government:[4]

> [W]e must make fundamental shifts in how the United States allocates roles, responsibilities, and resources in cyberspace. We must rebalance the responsibility to defend cyberspace by shifting the burden for cybersecurity away from individuals, small businesses, and local governments, and onto the organizations that are most capable and best-positioned to reduce risks for all of us.

The U.S. national cybersecurity strategy includes a key objective to “shift liability for insecure software products and devices,” flagging the fact that vendors currently “ignore best practices for secure development [and] ship products with insecure default configurations.”[5]

In the EU, the Cyber Security Act[6] (CSA) has tasked ENISA with issuing cyber security schemes and prescribes that such schemes should be designed to ensure that “ICT products, ICT

[3] https://www.cisa.gov/resources-tools/services/secure-cloud-business-applications-scuba-project.

[4] FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy | The White House.

[5] National-Cybersecurity-Strategy-2023.pdf (whitehouse.gov).

[6] L_2019151EN.01001501.xml (europa.eu).

services and ICT processes are *secure by default* and by design" (see Article 51). The CSA is clear on what the concept of "security by default" entails (see recital 13):

> Undertakings, organisations and the public sector should configure the ICT products, ICT services or ICT processes designed by them in a way that ensures a higher level of security which should enable the first user to receive a default configuration with the most secure settings possible ("security by default"). Security by default should not require extensive configuration or specific technical understanding or non-intuitive behaviour on the part of the user, and should work easily and reliably when implemented. If, on a case-by-case basis, a risk and usability analysis leads to the conclusion that such a setting by default is not feasible, users should be prompted to opt for the most secure setting.

The draft EU *Cloud Services Scheme*, issued by ENISA,[7] follows this principle, but it acknowledges that the responsibilities between cloud service providers and cloud services customers are split, whereby the scheme aims "at verifying that this split is explicitly and publicly documented by the provider." Cloud providers therefore have the option to specify any "*Complementary Customer Controls*," which for purposes of the certification count towards the provider meeting the relevant security standards.

For products with a digital component, the proposal for an EU Cyber Resilience Act[8] requires these to "be delivered with a secure default configuration, including the possibility to reset the product to its original state" (see Annex I Essential security requirement 1 sub (3)(a)).

Though this legislation is a big step forward, it is still very product-focused, and makes it possible for providers to label certain controls as "Customer Controls," avoiding the obligation to provide these by default. In addition, secure configurations are considered as static, in the initial status upon delivery of the product. This notion would not cover maintaining and updating configurations, controls, and policies throughout the lifetime of a product.

The status

Complaints about the complexity for users of the security configurations and controls of the cloud offerings of Big Tech are not new. Unsurprisingly, Big Tech itself is increasingly referring to the concept of security by default (see examples below). These efforts are commendable, but our concern is that they are not widely known, are not comprehensive (do not cover all products and services), are hard to understand, and are expensive to implement and maintain. They are product-specific and mostly present guidance rather than actual implementation by default.

Security by default currently seems for Big Tech like an afterthought, is treated in an anecdotal rather than a strategic way and is not sufficient to guarantee a minimum level of security.

- Microsoft *Secure Future Initiative*[9] [10] aims to "deliver software that is secure by design, by default, in deployment, and in operation." Though the scope of the initiative seems broad,

[7] EUCS – Cloud Service candidate cybersecurity certification scheme.pdf.

[8] Eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0454.

[9] https://blogs.microsoft.com/on-the-issues/2023/11/02/secure-future-initiative-sfi-cybersecurity-cyberattacks/.

[10] https://www.microsoft.com/en-us/security/blog/2023/11/02/announcing-microsoft-secure-future-initiative-to-advance-security-engineering/.

review shows that the focus is product-specific, does not cover all products (not included are, for example, Microsoft 365 and Edge), and is limited to specific elements of security (MFA, identity protection, key management, cloud vulnerability management). The Initiative further explicitly aspires to "Implement our Azure tenant baseline controls (99 controls across nine security domains) by default across our internal tenants automatically," but these are currently not released. The Azure built-in policies[11] constitute guidance rather than actually being built in.

- The Google Cloud *Shared Fate Model*[12] explicitly states that its model is based on Security by Default: "providing multiple levels of complementary defenses designed to reduce your risk for configuration errors as well as attacks." It refers to encryption for data at rest/in transit, DDoS protection, and default configurations for computing and storage to limit public access. Enterprise Foundations Blueprints[13] provide security guidance. Review shows that also here there are product gaps in the current security by default approach (not included are, for example, Google Workspace and Chrome) and listed features (like customer key management) are premium options and not implemented by default.
- Amazon makes available tools to "build secure, high-performing, resilient, and efficient infrastructure"[14] and to "assess the environment against security industry standards and best practices."[15] AWS Security Best Practices for S3[16] and the AWS Startup Security Baseline[17] provide guidance rather than actual implementation. There are no obvious references to implementation of security by default.

A new approach

Where most user organizations struggle with configuring infrastructure and ensuring and maintaining proper protection, Big Tech can do this according to the state of the art and at scale. We call upon these companies to look at their user base worldwide as an enterprise to be protected and apply baseline enterprise cybersecurity and resilience principles by default, including by using key controls and publicly reporting Key Control Indicators.[18] **This does not preclude vendors offering security solutions, integration, and services, on top of and beyond the baseline.**

Below we provide examples of implementations of configurations and controls which should be implemented by default. These examples are for illustrative purposes only. A comprehensive review and implementation of key controls/measures is needed. As indicated before, this does not require a ground zero effort. There exists a wealth of guidance on secure baseline controls issued by the national cybersecurity centers (CISA,[19] [20] ACSC,[21] CCB[22]), and specialized organizations (CIS,[23] CSA).[24] Big Tech has initiatives that help implementing such

[11] https://github.com/Azure/azure-policy/tree/master/built-in-policies.
[12] https://cloud.google.com/trust-center/security.
[13] https://cloud.google.com/architecture/security-foundations.
[14] https://aws.amazon.com/architecture/well-architected/.
[15] https://docs.aws.amazon.com/securityhub/latest/userguide/what-is-securityhub.html.
[16] https://docs.aws.amazon.com/AmazonS3/latest/userguide/security-best-practices.html.
[17] https://docs.aws.amazon.com/prescriptive-guidance/latest/aws-startup-security-baseline/welcome.html.
[18] https://www.researchgate.net/publication/374061802_Ten_Key_Insights_for_Informed_Cyber_Oversight.
[19] https://www.cisa.gov/cross-sector-cybersecurity-performance-goals.
[20] https://www.cisa.gov/resources-tools/services/secure-cloud-business-applications-scuba-project.
[21] https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight.
[22] https://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework.
[23] https://www.cisecurity.org/controls/cis-controls-list.
[24] https://cloudsecurityalliance.org/research/ccm-lite/.

guidance. A prime example is US FEDRAMP.[25] [26] [27] A coordinated effort to define, maintain, and implement secure baselines by default may also help to reduce the burden of disparate regulatory oversight across the world.

Big Tech also has extensive visibility ("telemetry") on the adversarial infrastructure/modus operandi and user organizations' communications, allowing such companies to perform "active defense." This is already partly done in browsers,[28] leaked credential detection,[29] or blocking IP addresses.[30] More can be done, and some national cybersecurity centers have deployed active defense measures that could provide inspiration.[31] [32]

Examples of configurations and controls that should be implemented by default (and that are currently not):

- DMARC (Domain-based Message Authentication, Reporting and Conformance); strong TLS (Transport Layer Security) protocols; AV/EDR protection; and hardening of browsers (safe browsing, blocking password saving, blocking insecure plugins and executables, HTTPs).
- Removal of default administrator passwords; separating user from administrator accounts; automated patching and phishing-resistant multi-factor authentication. Limiting internet exposure (*e.g.*, of cloud instances) should be standard, forcing a deliberate decision to open.
- Applying the principles of Least Privilege and segmentation is another area in which Big Tech's detailed knowledge of their infrastructure and products allows the creation of a safe user environment by default instead of expecting every user organization to create one.

Ultimately the security by default settings should cover the entire suite of user infrastructure such as:

- Office automation, email, conferencing, file sharing
- Infrastructure management and automation
- Identity and access management
- Networking, remote access, browsers
- Data storage, provenance, analysis, co-pilots
- Data encryption at rest, in transit, and in computing
- Logging, backup, resilience

Many default configurations, controls, and policies can be implemented without prior user interaction. For others, some initial workflow would be required (like changing admin passwords, implementing lowest-privilege controls, etc.). Native logging and secure backup solutions would for many organizations be the best path to tick off important key controls in detection and resilience. However, the cost of implementing these is very dependent on the

[25] https://learn.microsoft.com/en-us/azure/compliance/offerings/offering-fedramp.
[26] https://learn.microsoft.com/en-us/azure/governance/policy/samples/fedramp-high.
[27] https://github.com/Azure/azure-policy/blob/master/built-in-policies/policySetDefinitions/Regulatory%20Compliance/FedRAMP_H_audit.json.
[28] https://safebrowsing.google.com/.
[29] https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-risks#common-questions.
[30] https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023.
[31] https://safeonweb.be/en.
[32] https://www.ncsc.gov.uk/section/active-cyber-defence/services.

user organization’s volumes and required retention periods. A variable (and transparent) cost model might be expected.

The new approach will require organizational changes at Big Tech, like the creation of a “*CISO User Infrastructure*” function to steer and oversee identifying, verifying feasibility, implementing, and updating baseline controls, configurations, policies, and defensive measures in the user infrastructure. These activities need to be performed in close alignment with the user community to assess impact and feasibility of the defaults and other options.

A three-tier approach could be taken:

1. Secure baselines implemented by default, at no additional cost.
2. If (1) is not possible, secure baselines implemented *by workflow*.
3. Transparently explained opt-in services (*e.g.*, logging and secure backups).

User organizations could still raise their protection to a higher level if they wish. Those opting out of secure baselines may expose themselves to a higher risk and additional scrutiny from regulators and insurers.

The way forward

Our earlier paper, “*Digital Sovereignty Is Impossible Without Big Tech*,”[33] described our assessment of the potential drawbacks of our proposal and we will not repeat those here.

Our dependence on cybersecurity is ever increasing and the risk of disruption is very real. Attempts to mitigate cyber risk to acceptable levels using a traditional, decentralized approach counting on goodwill, efforts, and expertise at every single user organization are doomed to fail. We believe that security by default is the way to go.

There are positive signals that security by default is gaining traction with providers and governments alike, although in a too-narrow product-oriented and static manner. We need to take these efforts to more ambitious goals. Obviously, we realize that publishing opinion papers like this will not be sufficient to make tangible progress. Achieving progress will require the committed involvement of many stakeholders:

- Leadership at the main providers (Microsoft, Amazon, Google).
- Leadership at their main customers, having the biggest leverage.
- Involvement of representatives of small and medium enterprises in industry associations and information exchange communities (ISACs). Their voice is important and will resonate with the policymakers in governments and parliaments.
- Policymakers and national cybersecurity centers in the EU and the U.S., which have already started to voice proposals in the same direction, although less ambitious. They will hopefully realize that their important policy ambitions will have a higher chance of success if security by default is implemented by Big Tech.

Ideally, the approach would progress by mobilizing forces in a natural way, by convincing and lobbying—and by leadership, vision, and commitment from the stakeholders. If that doesn’t work, regulation could still be an option.

[33] https://www.atlcom.nl/artikel-atlantisch-perspectief/digital-sovereignty-is-impossible-without-big-tech-a-call-to-action/.