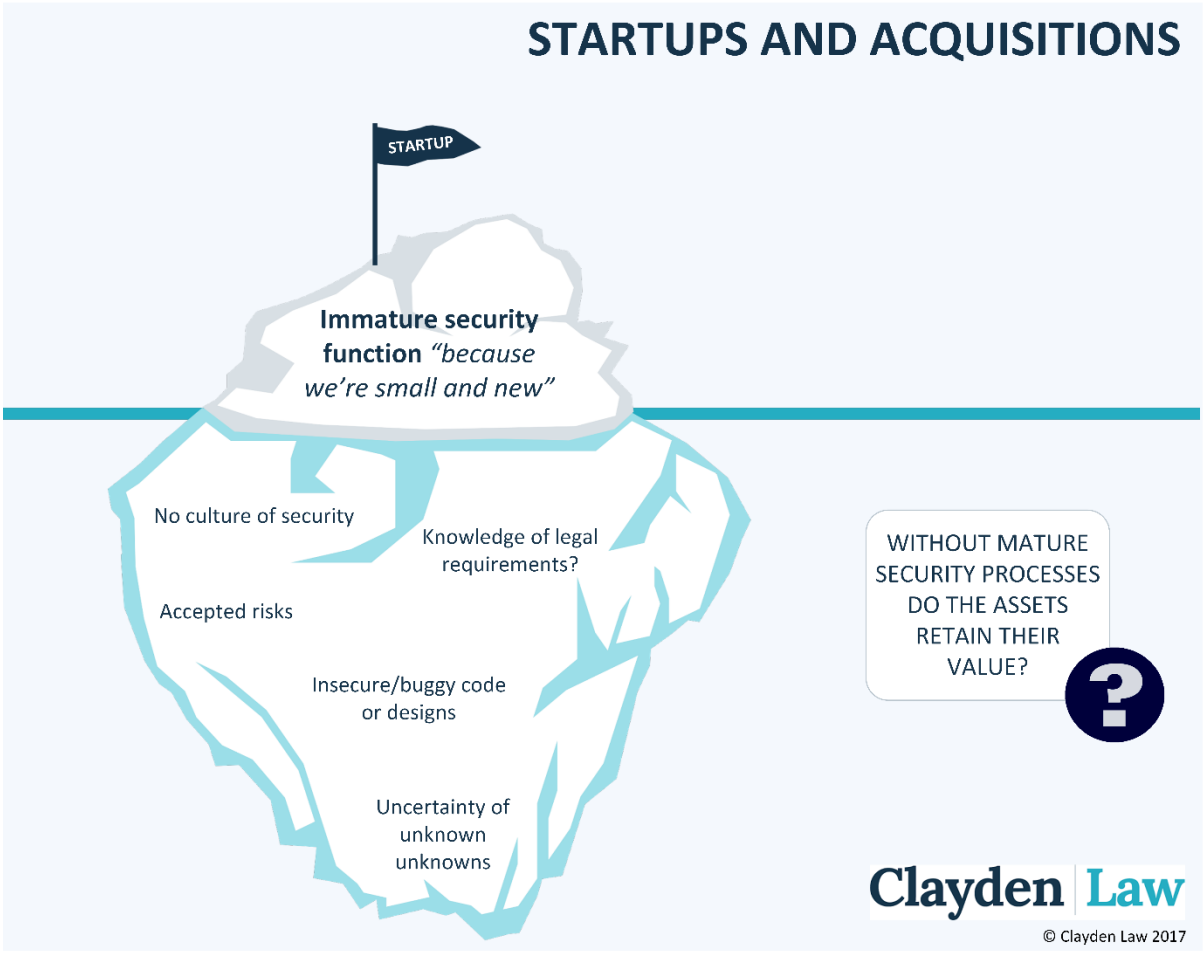
Clayden | Law

CYBERSECURITY SERIES: STARTUPS & ACQUISITIONS



Typically we discuss cybersecurity from the perspective of a mature organisation that needs to reduce specific risks. The company may have developed new business lines, or existing business lines may have evolved to be reliant on technology, but any security decisions have to be compatible with existing business processes.

In contrast, new organisations have to decide how to engage with cybersecurity in parallel to the development of all their other functions. In slow-growth organisations, cybersecurity may not hit the radar for an extended period, with founders focusing on establishing revenue-generating processes while relying on the security they use at home and secure defaults. Over time, they may become more security-aware and begin introducing more of the basic measures advocated by standards such as Cyber Essentials.

This is probably the pragmatic approach for these slow-growth organisations, assuming it is not in contravention of data protection rules. However, this approach is less applicable to startups intended to grow quickly, attract venture capitalists and eventually become a saleable asset.

In technology-driven startups, the quality of the codebase becomes a key factor in due diligence and cybersecurity becomes relevant from the outset. These organisations face the mammoth task of transitioning from a proof of concept to a robust product, future-proofing their processes against potentially exponential growth and proving the company's value to potential investors.

With technology-driven concepts, cybersecurity and legal frameworks (from data protection to the regulation of financial services) need to be intrinsic design considerations and purchasers should be wary of startups without evidence of cybersecurity policies and strategies.

SECURE BY DESIGN

Secure by design is more than a buzzword: organisations built for acquisition need to have robust security processes compatible with the larger organisations who may wish to acquire them.

The typical non-technical business founder hears the word cybersecurity and thinks about the layers of security their IT team use to stop unwanted guests having access to their network. At this point they may have no customers and feel that the intellectual property held by the company is not of the magnitude to warrant any particularly advanced security measures (or more likely, that their small team lack the time to implement new measures and the company lacks sufficient funds to invest in enough security to make a difference).

If the company is being built for acquisition it is important to introduce more advanced and easily auditable cyber security processes than those typically seen in a small organisation. Unfortunately, ensuring the confidentiality of the organisation's intellectual property is not the only type of cybersecurity a founder needs to be aware of from the outset.

Firstly, software developers will be the first to tell you that proof of concept code, as well as processes for managing the codebase and collaborating, never get entirely rewritten in each iteration of the development process.

Even when the founders are pushing to have something on screen for potential investors to see, they need to consider whether their software development team are putting sufficient emphasis on secure development practices. Agile development processes are in direct conflict with cybersecurity best practices and business owners need to be aware of the risks around a *build now, fix later* strategy.

Nobody wants to realise man-years into the development process that one botch or customised platform used in the "throw away" proof of concept code is going to stop the software ever being able to integrate security updates.

The company also needs to begin considering security as part of the design process in a sustainable way. The services offered by the company may require additional security once the company begins gaining customers. Data security tends to be planned based on the sensitivity of the data *and* its quantity (in line with data protection best practices).

In a startup projecting rapid growth this presents a challenge – some security measures introduce latency, which may become noticeable for customers should the service not be designed for scalability. More importantly, when the system is designed, if the security architect suggests 'adequate' security measures for a database of 1000 sensitive records and then the dataset grows exponentially, it is unlikely that the security measures will be indefinitely adequate. The value of an asset to an attacker (and so the threat), as well as the number of people impacted by a breach, grows with the size of the dataset. In the context of a rapidly growing startup, security needs to be designed with the intention that it is adequate for/can scale to a particular lifespan (and for the projected number of customers within that lifespan).

Beginning as you mean to go on also helps to ensure that security policies become part of company culture – making it more likely that an auditor would be able to give a startup credit for working towards standards such as ISO 27001, even before they are large enough to warrant attempting accreditation. While an organisation's processes will not be identical to that of its purchaser's, being able to show a level of security capability that makes them safe to merge with could significantly increase saleability and value.

PRIVACY BY DESIGN

The General Data Protection Regulation (GDPR) advocates privacy by design. Some elements of privacy regulations directly translate into cybersecurity requirements, while others influence the system design to ensure that data subjects' rights are protected.

The Information Commissioner's Office lists the following benefits to a privacy by design policy[1]

- *"Potential problems are identified at an early stage, when addressing them will often be simpler and less costly."*
- *"Increased awareness of privacy and data protection across an organisation."*
- *"Organisations are more likely to meet their legal obligations and less likely to breach the Data Protection Act."*
- *"Actions are less likely to be privacy intrusive and have a negative impact on individuals."*

Most importantly for startups needing to be ready for the GDPR, it includes Privacy Impact Assessments (PIAs). This means that as well as considering carrying out cybersecurity risk assessments with the aim of protecting shareholders' assets, the company needs to carry out similar assessments for each dataset that includes personal data within the organisation; *from the perspective of the data subject as a risk holder* (risk was discussed in more detail in a previous publication).

Another thing for consideration is the ability to show due diligence where GDPR is concerned, prior to acquisition.

Let's assume that the startup carried out a risk assessment including PIAs and spent their budget reducing the most impactful, most likely, risks. *All* organisations end up with residual risks and it may seem logical for the startup to retain an expensive risk, which has a low likelihood of happening, because the mitigations would cost more than the fine.

With the evolution from a fixed maximum penalty to a percentage of annual global turnover, this risk calculation is likely to be different from the perspective of the acquirer. It doesn't mean that the startup has made the wrong decision, but it is something a purchaser needs to be aware of to prioritise any technical or organisational changes they need to make at the point of purchase.

ACQUISITION

As stated in the previous sections, cybersecurity and privacy considerations are becoming increasingly relevant to the due diligence companies carry out prior to acquisition. There are a number of issues

1 ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/

involving the technical elements of a company that should be considered when valuing its assets. These include:

1. The value of the in-house software or data assets.
2. The maturity and culture of their technical business processes.
3. The risks that they have identified but have had to accept.

In terms of the value of the technical assets, there are many issues that can influence a valuation. These might include the quality of the code (to what extent it is proof of concept code that would need to be rewritten more securely? Does the dataset include the records of consent that make it legal to hold personal data?), the uniqueness and confidentiality of a dataset (does it give the purchaser a competitive advantage?) and the resiliency of the system these assets resides in (could the assets be lost due to lack of recovery planning between purchase and system upgrades/transfer of data?).

All of these examples have a link to cybersecurity practices and are influenced by the culture and risk appetite outlined in 2 & 3. A low level of maturity in cybersecurity or privacy related processes may indicate a broader-reaching problem that will influence the value of the assets – if the in-built free firewalls on the router have not been activated and configured is the technical team also unaware of vulnerabilities that may have been introduced by their code? If employees regularly communicate with each other using gifs and memes do they understand the risks of introducing malware into the corporate network and its potential sources? If the overall level of cybersecurity is low then has the organisation adequately evaluated the legal responsibilities (privacy-related, financial, due care in service provision) they take on with the system they have built? Also, since the likelihood is that privacy regulator interest is more likely than not to be piqued by a security breach notification, (and that interest may lead the regulator to take a closer look at the general compliance picture of the company) getting cybersecurity right takes on an even greater importance.

Cysbersecurity risks aside, how about the functionality of the software itself – will it be able to handle the increased bureaucracy and process-layer required to enable the provider to response to requests from individuals exercising their new enhanced rights under GDPR, such as the erasure right and the right to restrict processing.

More generally, any potential purchaser will also want to flesh out in the due diligence process the risk of potential data protection liabilities and will want to evaluate those risks. Start-ups sitting on large data-sets which are to some extent driving value will want to show that those data-sets have been created in a privacy compliant way to ensure continued use. At the risk of stating the obvious, companies which have a messy privacy compliance picture are likely to achieve lower valuations these days in light of the hugely increased financial downsides (regulatory fines, individual claims and loss of reputation) in getting it wrong.

Finally, are the risks the company has had to accept compatible with an acquisition? Would the system require immediate remediation at the point of purchase? Known risks and limitations faced by a smaller organisation may change the price of a company, but would not make it unsaleable. However, indications that cybersecurity has been systematically non-prioritised within an organisation may indicate that the known issues are just the tip of the iceberg. The potential for cybersecurity unknown unknowns is quickly becoming a deciding factor in the price a company can achieve.

ROUNDING UP

Clayden | Law

Different business models have different requirements when it comes to choosing how to implement cybersecurity. Startups should be a special case when it comes to cybersecurity. Although it is common practice for cybersecurity capability to mature as an organisation grows, startups founded with the intention to sell need to be considering cybersecurity and privacy best practices from the outset, and investing in rigorous policies and processes as soon as it becomes feasible.

Organisations intending to purchase startups, especially those with technology-heavy business lines, need to be considering cybersecurity and privacy policies and practices as a key factor in asset valuation.

Please be aware that these notes have been compiled for general guidance only and should not be considered as specific legal or technical advice.

Piers Clayden, piers@claydenlaw.co.uk
Founder & Director, ClaydenLaw