

SOCURA

TRICKERY



RIGIDITY



LETHARGY



DENIAL



DECEPTION



INEPTITUDE



GLUTTONY



7 DEADLY SINS

OF CYBER SECURITY SERVICES



DISTINGUISH THE GOOD FROM THE BAD

As with any service industry, there are as many bad cyber security services companies as there are good ones. Unfortunately, the stakes are extremely high for organisations in this market. Being able to distinguish the good from the bad can be the difference between a majorly disruptive and costly data breach, and a business-as-usual workday.

There are some tell-tale behaviours exhibited by the least trustworthy, effective, and reliable cyber firms. These are the seven deadly sins of cyber security services and how to counter them.



DECEPTION

Deception features top on the list of security shortcomings, because of its prevalence and seriousness. Deception rarely means outright fraud; It is more common for organisations to lie and hide issues. Consider failure to provide adequate auditing or visibility in this category. This kind of deception or obfuscation is usually the tip of the iceberg, used to cover up for mistakes, bad human processes or limited technical capabilities.

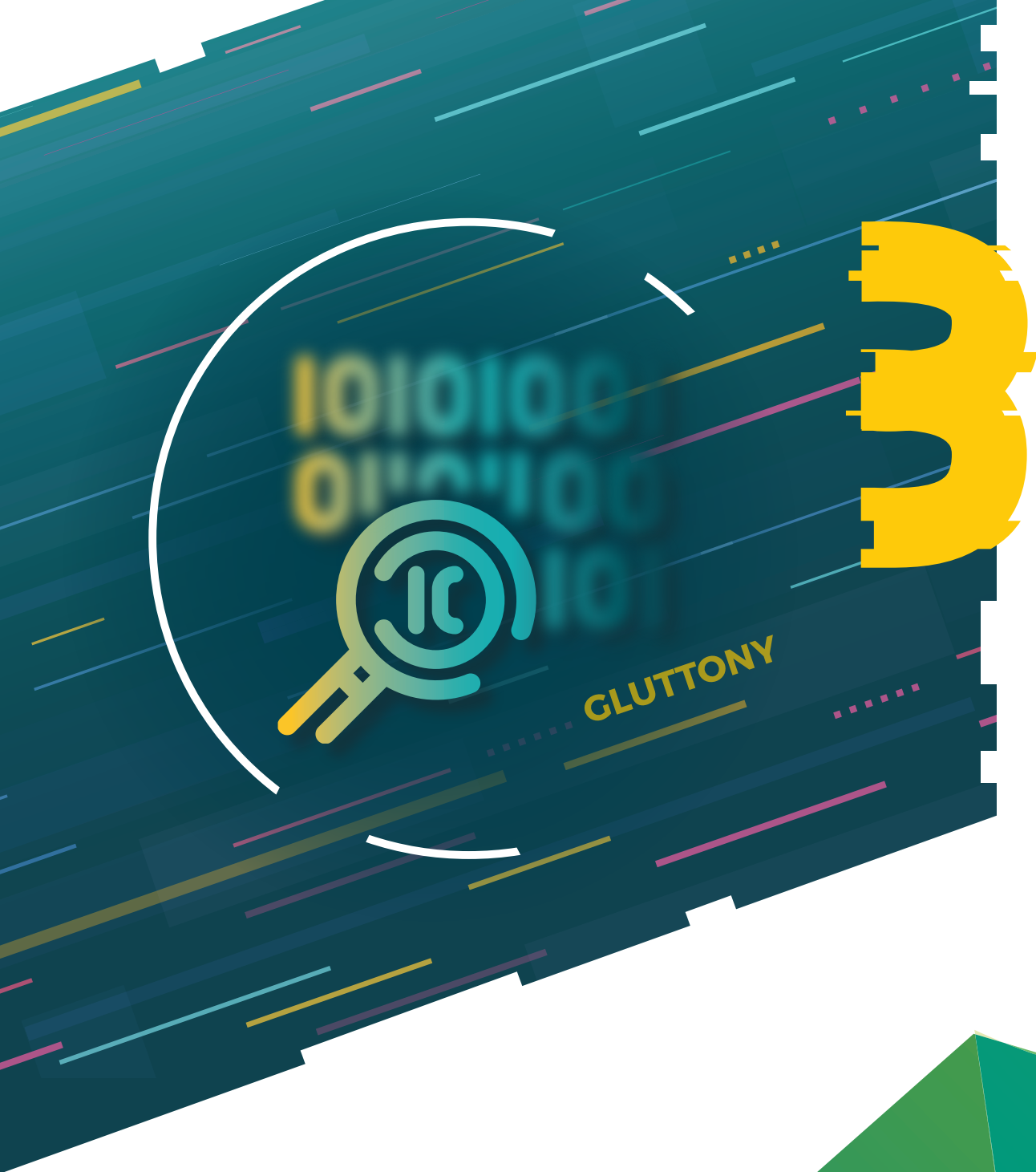
Any kind of deception can destroy trust, which is a vital and precious commodity in cyber security. Once it is lost, it is difficult to regain. Customers who feel like their cyber security partners are not being 100% truthful with them should press for transparency and more detailed reporting. They should run a mile if they can't get it.



INEPTITUDE

The aptitude of a security partner should not be a binary good/bad based on outcomes alone e.g. whether they prevent a breach. Businesses must learn to identify the good from the bad in other ways. For example, lacking organisation, providing an inconsistent service, or failing to follow through on the service, timescale, or budget discussed. It should not take a data breach, missed alert or serious incident to realise that an organisation offers a poor standard of service.

Companies should demand their security partners be organised, consistent, and follow through on their commitments. Partners must communicate clearly with their clients, set realistic expectations, and work to deliver on those expectations.



GLUTTONY

Sadly, many cyber security companies operate with the mantra, “If it’s not in the contract, it’s chargeable.” These companies will often have hidden fees, and their work will cost more than expected or quoted. If they do make changes to the contract with a client, it is often at an exorbitant rate.

There needs to be more pricing transparency from cyber security service providers, but there is also an onus on customers to look out for hidden fees and dodgy deals. If a quote seems too good to be true, it probably is.



4

LETHARGY

Some security teams are more engaged and proactive than others. Companies should be extremely wary of cyber security partners that provide contractual agreement services to an acceptable quality but put in the bare minimum effort elsewhere. These companies provide a poor-quality service for anything that is not in the contract, such as availability to attend meetings, delivery turnaround of requests for information, or other requests.

If they are lazy, slow, unresponsive, or unsupportive in their day-to-day work, can you really trust them in scenarios where you need your security partner most?





RIGIDITY

It is remarkable that in such a dynamic industry, some cyber security companies are completely inflexible.

These companies have their desired processes, and everything must be done in their preferred format. This often wastes the customer's time, and it ignores the nuances of the industry. This is a sin of customer service, because it demonstrates that a partner prioritises their processes over the needs and time of their customers. Customers should be careful of partners who are not as accommodating as they should be, because the experience of working with them may be frustrating.



TRICKERY

Security firms that are willing to trick their customers and do things behind their backs. For example, they may remove items from their Service Improvement Plan, Actions registers, etc. without consent. They either convince the customer that it is not required anymore, or the item hasn't been on the list for so long that the customer has forgotten about it.

These tricks leave a sour taste. They are avoidable and often unnecessary. The customer may well be happy to make changes if they are consulted and guided in advance.





DENIAL

While it's important for cyber security professionals to push back against client demands, when necessary, some partners take it too far and say "no" to everything. This can be harmful to the customer, who may feel that their needs are not being taken seriously. Providers need to find ways to say "yes" more often and be more accepting of their customers' needs and challenges. For customers, if you are always at odds with your security partner, it may not be a good fit for either party.

Organisations need to do thorough research before choosing a cyber security provider, reviewing their reputation and customer reviews. If a security partner is guilty of the sins above, it is worth searching for a more suitable match immediately. It's important to remember that the cost of changing partners pales into significance vs the cost of a data breach.

The Value of MDR

This is where extended detection and response (XDR) and managed detection and response (MDR) come in. MDR is increasingly favoured, as building and manning a 24x7 security operations centre (SOC) in-house is hard to justify from a cost perspective. Organisations can instead utilise the economies of scale that a specialist provider offers, and the enhanced visibility they have into multiple customer environments.

For health and care leaders, MDR offers:



24x7 threat detection and response across remote, endpoint, network, cloud and OT environments.



An extension of your security team, freeing up in-house resource to be more strategic.



Rapid response to mitigate threats before they have had a chance to impact the organisation.



Swift detection and containment provides an extra layer of defence, because prevention can't catch everything.

However, in a fast-growing market, not all MDR services are created equal. Many, for example, are limited by the amount of data they can store, retain and analyse, which can impact their efficacy.

Here are three questions to ask of a prospective vendor:

- 1 How much security data do you collect, and is this cost-constrained?** Telemetry must be collected from every asset/device, and across all parts of the IT infrastructure (including IaaS, PaaS, SaaS, endpoints, firewalls, email, directory services, DNS, Proxies, VPN, etc). Data should go back a year for maximum visibility.
- 2 By how much can you reduce attacker dwell time?** Modern threat actors often move fast. You need to reduce dwell time from days or hours to minutes through threat hunting, automated containment actions, and pre-approved playbooks.
- 3 How closely will you work with my existing security team?** The best providers will work seamlessly as an extension of your in-house team, with a dedicated security analyst and customer success manager.

If you would like to find out more about how we can help you, **please contact the team at hello@socura.co.uk**

Why Socura

We're here to help make the digital world a safer place and change the way organisations think about cyber security. We blend our technical expertise and industry experience with a people-centric approach and work right alongside our clients to guide them along their cyber security journey.

It's our people-centric approach that truly sets us apart. We like to keep it simple, distilling this into 3 core values:



Share the Journey

Knowing that wherever you are on the journey, we're right there alongside you, and only ever winning when you are.



Be the Light

Sharing our knowledge and insight to empower your people and light the way to a smarter, more effective security approach.



Make it Count

Making every interaction count, filtering out the noise and delivering true value on the things that matter most, every single time.



Crown
Commercial
Service
Supplier



National Cyber
Security Centre



HM Government
G-Cloud
Supplier

