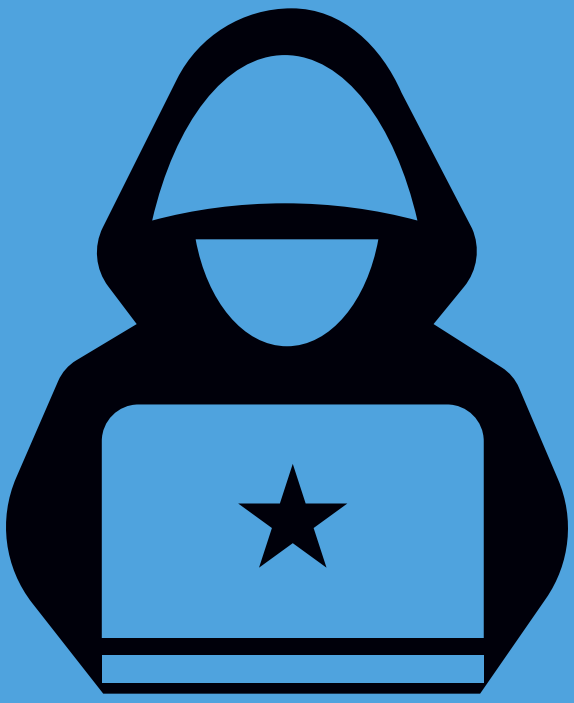
SysAid®



5 REASONS THE SERVICE DESK SHOULD CARE ABOUT INFORMATION SECURITY

By **Stuart Rance**, *ITSM and security consultant*

In many organizations there is a separate information security team that deals with all things relating to security. This team is responsible for designing and implementing all the controls needed to protect the organization, and for managing all major security incidents. So why does the service desk need to be involved, and what contribution should it make?

Here are five reasons that you should consider:

1. Everyone's Responsible for Security

The first and most obvious reason is that information security, also known simply as InfoSec, isn't just about process controls or technology controls that we can delegate to the InfoSec team and then ignore unless they affect us directly. Good information security depends on a good balance between people, process, and technology controls, where the people controls affect a broad range of personnel in the organization – all of whom need to take some responsibility for security.

Service desk agents, like everyone else in the organization, need to know what information security policies apply to them, and need to take responsibility for following these policies. Typical policies that everyone needs to follow include:

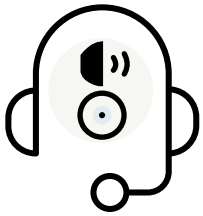
- **Acceptable use policies** – what you are allowed to do with email, social media, the company network, etc.
- **Mobile device or BYOD policies** – how personal devices such as laptops, tablets, and smartphones should be managed
- **Password management policies** – how often you have to change your password, rules about how passwords are made up, and whether you're allowed to record passwords
- **Remote working policy** – rules for how people should work from remote locations, such as their home or a hotel room
- **Information classification and handling policies** – how documents and other information should be classified, labelled, and handled; for example: certain types of information may not be transferred out of a secure location, other types of information must always be encrypted, etc.
- **Visitor policies** – how visitors to your site should be managed

Your organization probably has lots more InfoSec policies that should be followed by all staff, so you need to find out what they are, and make sure your service desk staff understand and follow them.

2. Service Desks Are the Eyes and Ears of IT

Major security breaches at some organizations have remained undiscovered for many months, during which time the attackers have been able to make off with vast amounts of highly confidential data. Early detection is crucial.

Your service desk is the main interface between the IT organization and the people who use your IT services. This means people who work on the service desk are uniquely placed to understand what is happening within your user community. If they are appropriately trained, they can be a first line of defense against many potential security breaches.



For example, issues such as users being locked out of their accounts for no obvious reason, data being deleted or data integrity being compromised, and performance problems due to unusual system and network usage can all be early signs of something more serious. If your service desk staff have been trained to consider such issues, they may notice the very early signs of an attack and escalate this to the appropriate InfoSec team. By helping you to identify security incidents quickly, your service desk can help change a major incident into something more manageable.

3. Service Desks Can Communicate Information Security Messages to Users

The service desk is in regular contact with users, and you can use this as an opportunity to communicate essential InfoSec messages, to reinforce other training and awareness activity.

For example, you could put a banner message on your self-help portal reminding people never to copy confidential data to portable media, or you could include a permanent message, with the email you send asking a user to complete a post incident survey, about never sharing passwords.

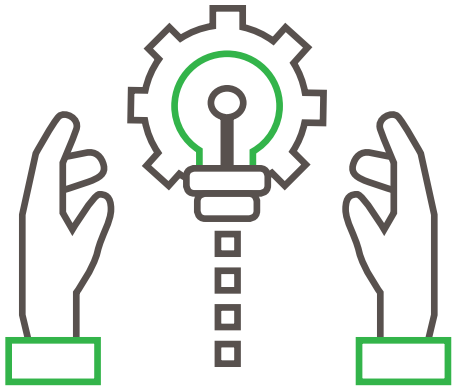
This is a great opportunity for service desk management to collaborate with InfoSec staff, planning how they can help communicate essential messages, and building relationships.

4. Service Desks Have a Major Role to Play in Security Incident Management

Most organizations have a security incident management process that is designed to:

- Log, track, and manage security incidents
- Escalate security incidents to people with appropriate skills and management responsibility
- Triage incidents and implement an initial response to contain the damage and stop it from spreading
- Ensure that confidential information about security incidents is suitably protected
- Preserve evidence that may be needed in case of legal or regulatory involvement
- Investigate and resolve security incidents
- Communicate with stakeholders such as police, regulatory authorities, shareholders, and the press
- Carry out post incident reviews to learn from the security incident

It's very hard to get all of these things right without practice, so a good InfoSec team will run rehearsals and simulations to ensure that everyone involved is ready and able to take the right action when an incident happens.

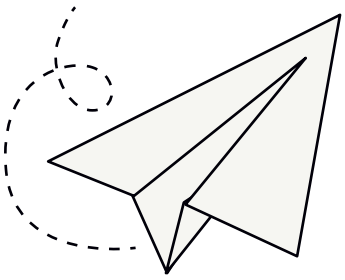


The service desk is often the first place to become aware of security incidents, so they have a major role in this process flow. In some organizations, the service desk will also be responsible for logging, tracking, escalating, and managing security incidents. In all cases, the service desk should be involved in the rehearsals and simulations, to ensure that they know what is expected, and to make sure they get it right when a real attack happens.

5. Service Desk Staff Are Role Models

Service desk staff deal with users when things aren't working properly, giving advice and asking questions. It is important that they are trained to do this in a way that demonstrates behaviors you want to encourage, and avoids any behaviors you want to discourage.

If service desk staff ask users for their passwords, then this implies that it's acceptable to share passwords, which may later make it easier for an attacker to trick people into giving out their passwords. If service desk staff send executable files by email, or ask users to click on a link to sign in to their accounts, then this will make those users more likely to fall for a phishing attack.



There are still some organizations where the service desk staff need to ask users for their passwords, in order to troubleshoot incidents or to build new computer systems. If this is your situation, then you urgently need to get new tools and redesign your process so that you can stop doing it. You can't afford to consistently demonstrate the wrong behavior to your users, because it encourages them to do the wrong thing too. After all, you don't really want train your users to give out their passwords to anyone who sounds sufficiently plausible, do you?

Summary

Don't just leave information security to your InfoSec team. Your service desk staff can play a big role in helping to protect your information if you give them the skills, knowledge, tools, and training they need to play their part.