THE ITAM REVIEW

ITAM in the Ascendency

Strategic Stakeholder Management

AJ Witt

servicenow

Executive Summary

A key finding from The ITAM Review's recent **user survey** [1] is that ITAM is in the ascendency. We're gaining traction with senior leaders and increasingly seen as an essential function for enabling digital transformation. ITAM teams are uniquely placed to provide a holistic view of the IT landscape through their people, processes, and tools. This holistic view improves strategic decision-making, helps break down silos, and identifies opportunities for innovation and service improvement. This whitepaper provides a roadmap to enable ITAM teams to gain seniority and contribute enhanced business value through effective stakeholder engagement. Practical examples are provided for engaging with frontline IT, Security, and strategic stakeholders such as Business Analysts & Architects.

Table of Contents

IT Leadership Priorities

Let's begin by reviewing some of the key trends in IT Management, as this will help us strategically align our activities with the priorities IT senior leadership are focused on.

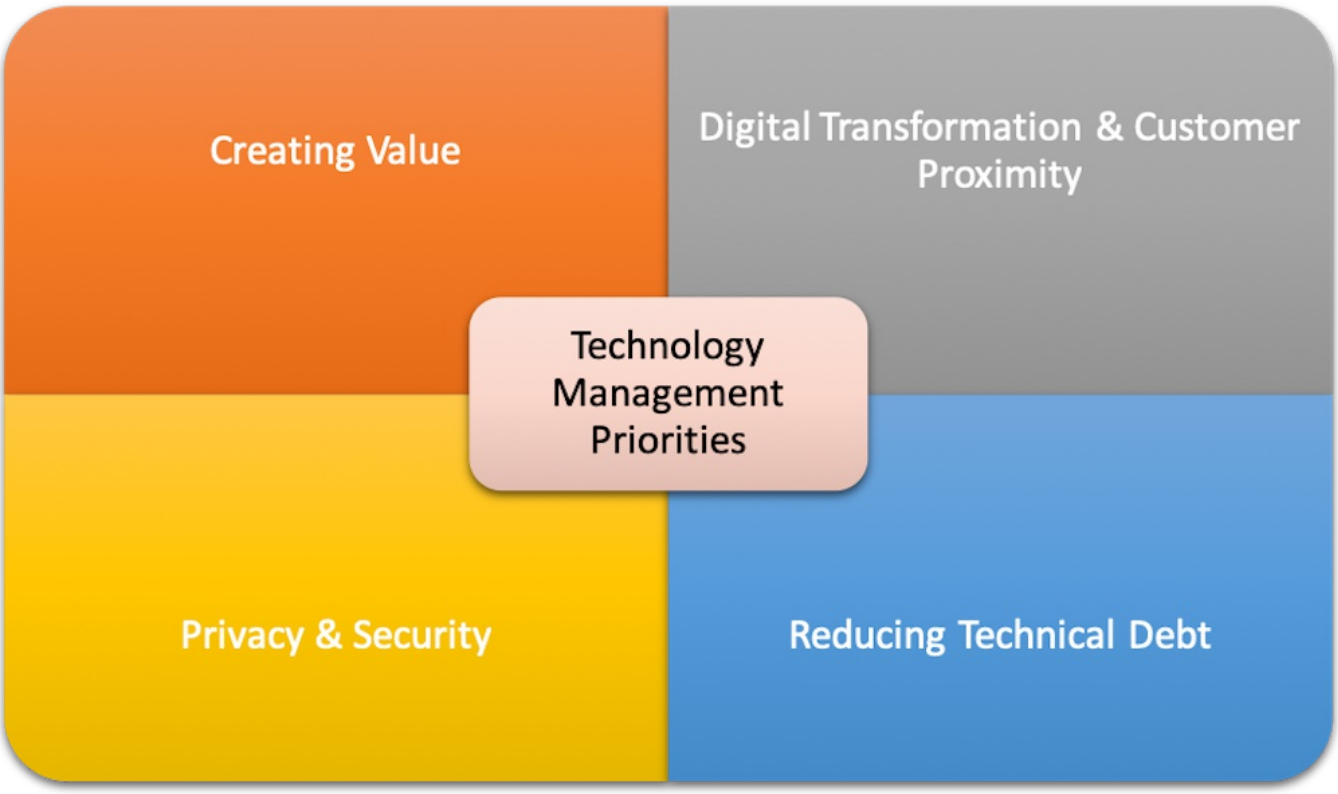

Fig 1: CIO Priorities 2019

Trend 1: Creating Value

The recently-released ITIL 4 standard has a strong focus on understanding and quantifying the **value chain** [2] delivered by a business process, system, or investment, as does the IT4IT standard. This builds on ISO standards for ITAM (ISO 19770) and also ISO27001 (Information Security Management). With so many organisations now standing on digital foundations, looking at value creation as well as cost & risk is an important shift in mindset for IT Management teams.

Trend 2: Digital Transformation & Customer Proximity

Digital Transformation is putting technology at the heart of everything your organisation sells – be that a physical device or a customer service AI bot. The technology we manage is closer than ever to the end consumer. It has become the means of production & value generation. Digital assets critical to value creation require the same level of continuous improvement, governance, and protection as a physical factory production line or supply chain. ITAM teams are well-placed to make a difference here and the proximity of technology to the customer makes Asset Management a strategic priority.

Trend 3: Privacy & Security

If technology is the means of production and value creation, then you'd better ensure that it's safe and secure. And if value generation depends on customers providing you with sensitive personal data then you'd better make sure you're complying with regulatory requirements such as the GDPR, and the upcoming California Consumer Privacy Act. Without that focus customers may choose to go elsewhere, or consumer protection authorities may even ban the **sale of your product** [3].

Trend 4: Reducing Technical Debt

CIOs continue to battle against the hodge-podge of legacy systems, a veritable Gordian Knot of interconnected systems creaking under the strain of years of under-investment. For a case study of what happens when the hens finally come home to roost, **look at the travails** [4] of UK bank TSB as they tried to implement a new banking system. Two weeks downtime, 80,000 customers lost to rivals, and a total charge of $450m. As with the **Equifax hack** [5], imperfect knowledge of interconnected systems and the steps required to restore service directly contributed to this failure, resulting in senior leadership resignations and a grilling from legislative committees.

What is the opportunity for ITAM teams?

A traditional ITAM team may have been tasked with reducing technical debt, or ensuring a value chain runs smoothly by being asked the question "What are we running where?" Something that probably your tools could answer authoritatively but leaves you as a bit-part player in a Broadway show.

The type of questions a Strategic ITAM team could answer are "How should we approach delivering this service for our customers?". You won't find the answer to that inside your team, or your ITAM tool, or even your processes. To answer that sort of question you also need to bring together stakeholders from across your technology function.

How do you do that?

Towards Strategic ITAM

Firstly, Foundational ITAM is still about People, Processes, Partners, and Tools, but critical to enabling this shift to Strategic ITAM is the ability to build strong stakeholder relationships both within and outside IT. Strong stakeholder relationships help ensure tools are implemented and running smoothly, that ITAM processes are integrated as part of business-as-usual, and that the right people & partners are doing the right things across the IT organisation and beyond. In doing this technology teams are enabled to deliver the right services and products to our internal and external customers. The starting point for this activity is the same ITAM lifecycle we're already familiar with; the difference comes in understanding the stakeholder requirements & benefits for each stage of the lifecycle.

The ITAM Lifecycle

An approach to the ITAM lifecycle many will be familiar with is as follows

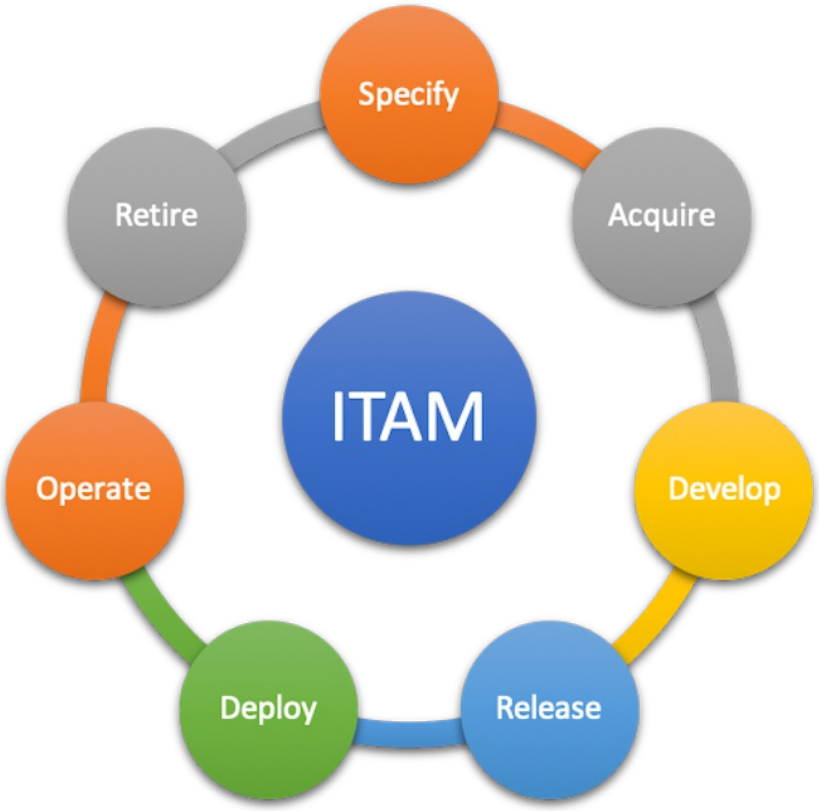

Fig 2: IT Asset Management Lifecycle

Each lifecycle stage will see an ITAM team working with different stakeholders. For example, HR will be a key stakeholder in the Joiners, Movers, Leavers (JML) process that forms part of Specify & Retire. Application Support teams will be key to Deploy & Operate, as will Security Operations. Acquire stakeholders will be Procurement & IT Financial Management, and so on.

ITAM is at the centre of all of this, and with our new focus on the value chain we must remember that the goal is that these activities create optimal value for our organisation and its external customers. It is our job as strategic ITAM teams to co-ordinate this lifecycle; to generate optimal value the best approach is to engage the required stakeholders, rather than try to do it all ourselves.

Taking a broader view, strategic, modern ITAM is more of a governance function than it is a day-to-day BAU function. Automation, Integration and AI is **already handling** [6] BAU tasks for ITAM teams. This is mirrored by the ongoing transition of IT as a whole from being a predominately hands-on technical department to a strategic value generator and centre of governance. IT departments respond to business demand and become as much of a production line for business value as a physical factory does. With technology becoming increasingly decentralized, the need to govern it centrally has never been more important.

Stakeholder Engagement

Key to becoming a strategic governance function is the ability to engage stakeholders in your mission. There is simply too much to do to deliver everything with a single team. Furthermore, doing so simply doesn't fit culturally with the rapidly evolving IT landscape of DevOps and Departmental (Shadow) IT.
This whitepaper focuses on key stakeholders internal to the IT function. These are your building blocks for strategic ITAM – with strong relationships in place at this level you can begin to extend your reach and impact.

Our key internal relationships are;

- End User Computing & ServiceDesk
- Security Operations
- Architects & Business Analysts

These map in to the ITAM lifecycle as follows:

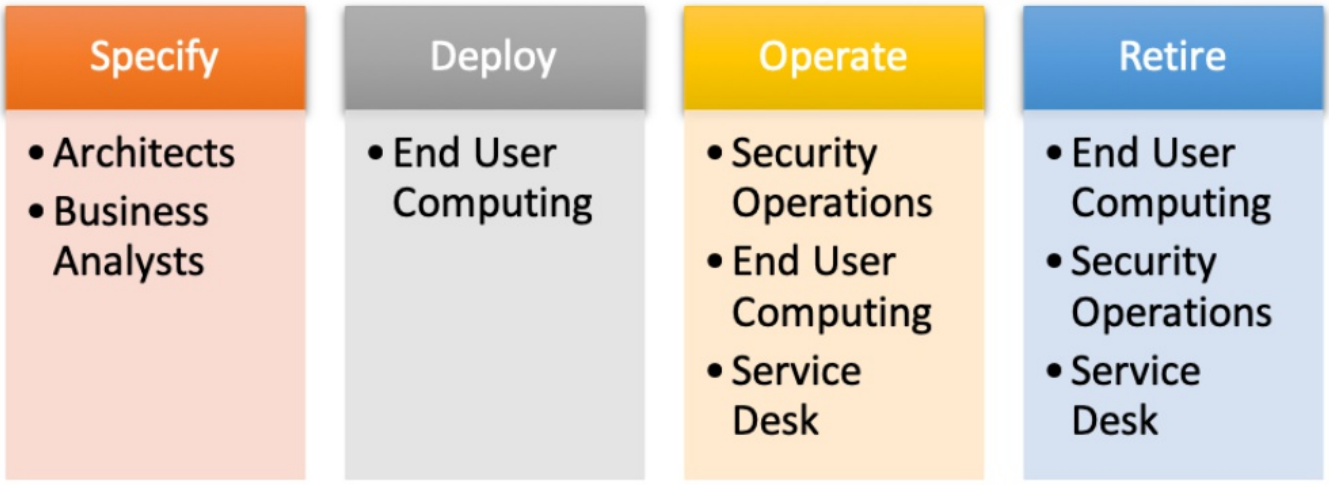

Fig 3: Critical Stakeholders by ITAM Lifecycle stage

N.B. The stakeholder list on the previous page is not exhaustive – it merely illustrates where the stakeholders we'll cover in the rest of the whitepaper sit in the lifecycle.

Specify

By getting ITAM embedded in IT delivery from the start – at the ***Specify*** stage – you're getting off on the right foot. Architects & Business Analysts are faced with many approaches to solving the same problem, and ITAM has a big role to play in modelling different solutions from a cost, risk, and value perspective. Your estate-wide view will considerably enrich decision-making at this lifecycle stage.

Deploy

The ***Deploy*** stage provides ITAM with the opportunity to deliver improvements in employee experience. By helping End User Computing & Service Desk meet their SLAs we can ensure license compliance, conduct license harvesting, and get employees the tools they need to do their job, when they need them.

Operate

The ***Operate*** stage has many stakeholders, but we'll focus on engaging Security Operations teams for mutual benefit. There is an **increasing focus** [7] on the power of ITAM, and particularly Discovery and Inventory, from Security Operations teams as they operate with the mindset of "you can only secure what you know about".

Retire

For ***Retire*** our main internal stakeholders are those we've covered in Deploy & Operate – Security Ops, EUC, and Service Desk. Increasingly, this area will be influenced by external stakeholders too – HR for offboarding, and employees – who are, in a world of SaaS, important decision-makers at this lifecycle stage.

Now that we've defined which stakeholders are the ones to prioritise at each lifecycle stage, let's do a deep-dive and look at how to engage each of them, starting with frontline IT – your Service Desk & End User Computing teams.

ITAM for EUC & ServiceDesk

Your End User Computing (EUC) & Service Desk teams are vital stakeholders for effective ITAM, working in the Deploy, Service/Operate, and Retire lifecycle phases. They're the people who get hardware and software in the hands of your users and are the public face of IT.

These teams often work in a high-cadence, stressful environment. Demands are constant, scale is large, and work is often unpredictable. As a function they are very much focused on the here and now. They manage everything from legacy apps to requests from users running shadow IT and provide service to everyone from the front desk to the C-Suite.

What they do

EUC & Helpdesk teams receive service requests from users for hardware and software. They process incidents relating to the entire IT infrastructure – everything from a forgotten password to a major service outage. They may be an in-house resource or be provided by a third party or managed service. They work very closely with users. They build strong relationships with the departments and users they serve, sometimes to the detriment of IT and the organization. It's common for support engineers to be socially-engineered by departments and individuals keen to get the latest kit, or bypass process to get software installed. Being young and ambitious they're often over-helpful, particularly for demanding users.

EUC & Helpdesk Team Managers seek to control this relationship in a number of ways. For EUC there may be a "Build Room" with controlled access, meaning users can't "drive-by" the engineers and put requests in. Helpdesk agents may only be contactable via a shared contact number. Most will have policies stating that all requests need a ticket logged before any action will be taken.

So that's the background. To dig a little deeper into what these teams do let's look at the Build process for deploying a new laptop.

The Build Process

What's involved in building a laptop? Build is split into the following phases:

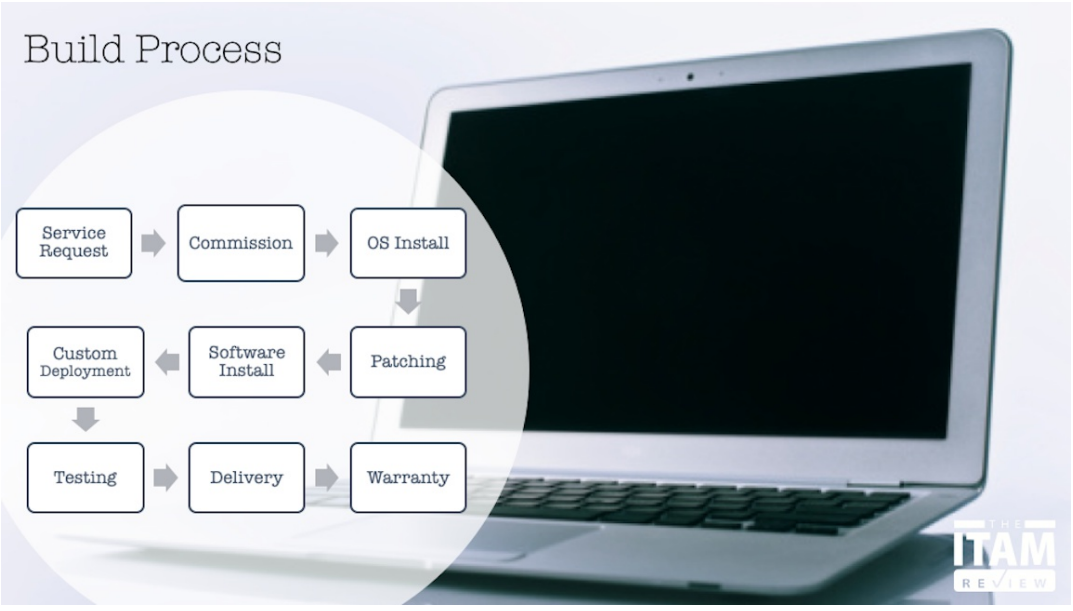

Figure 4: Build Process

- **Service Request** – the process for requesting and authorising acquisition of the laptop.

- **Hardware commissioning** – getting the laptop out of the box, powered on, and checked.

- **OS install and activation** – most organisations will deploy a custom Operating System image on their laptops, often referred to as a "gold master". At this point the domain computer account will be created and the laptop added to the domain. Automation has a role to play here, and in some cases larger organisations will receive kit pre-configured laptops with their master build installed

- **Patching and updates** – the pace of change is such that all laptops will need patching with security fixes and other updates.

- **Software Installation** – standard software packages will be installed and activated.

- **Custom deployment** – any "special-request" software not usually deployed widely in the estate – for example engineering software

- **Test** – typically the laptop will be left powered-on and connected to the network for a period of time to ensure there are no hardware or software issues.

- **Delivery** – the laptop is delivered to the user either by hand or by delivery

- **Warranty Support** – many EUC teams run a warranty period for newly-issued hardware whereby the user can receive priority support

ITAM vs EUC Priorities

Based on the above build process the priorities of each team can be summarised as per Figure 5:

Phase	EUC priority	ITAM priority
Hardware Commissioning	Check, Power On	Create the CI and have the hardware scanned by discovery, and added to the Asset Register
OS Install & Activation	Install OS, Activate, Add to Domain	Ensure OS is licensed
Patching & Updates	Bring laptop to a current, usable state	Run current software
Software Installation	Get the user the software they need	Ensure software is required & licensed
Custom Deployment	Complete special user requests	Ensure software is required & licensed
Test	Verify no hardware & software faults	None
Issue Laptop	User handover & check, request sign-off	Ensure machine is inventoried
Warranty Support	Ensure laptop is working	Ensure warranty information associated with the laptop is tracked during the lifecycle

Figure 5: ITAM & EUC Priorities

The Challenge

The Build process is time-consuming with a lot of moving parts and to-and-fro between EUC & the user. Often, EUC will have received the request late, and the user will need it to be completed yesterday. Anything that gets in the way of delivering that laptop will be short-cutted, incomplete, or just plain ignored. Whilst automation has an increasingly large role to play here, there is still manual intervention required and therefore risk of human error.

EUC teams operating in this way will inevitably build up license non-compliance positions. If they're measured on number of requests closed, licensing won't be checked. You need to ensure your engineers to meet ITAM objectives too – summarised as only installing authorised, licensed, required, and serviceable software.

Stakes in the game

So, how do you address this challenge? First, you need to add value for your frontline teams. Second, you need to find a way to align your goals and deliverables with theirs.

To recap, the key motivators for EUC Teams are;

- Getting the incident or request closed
- Getting the laptop built and issued quickly

Analysing this further, the needs of each stakeholder can be summarised as follows

- **Users** are happy when they get the laptop they want, with the software they need to do their job, delivered on-time
- **EUC Teams** are happy when a build is done quickly and efficiently using the right software
- **IT Managers** are happy when the above is done according to process and within budget
- **ITAM Managers** are happy when the asset is being inventoried correctly for HAM/SAM purposes and all software installed is in-use and no license compliance issue has been generated
- **CIOs** are happy when they receive positive reports regarding IT service levels and costs aligned to budget expectations

Bringing this all together we can see that there is an overlap in motivators and goals that can be further summarised as follows:

All stakeholders are satisfied when laptops are built and delivered on time & cost & risk is minimised.

ITAM Processes & Procedures are essential to enabling this outcome. Read on for practical tips on how ITAM empowers EUC customer service.

ITAM Processes & Procedures for EUC

The following are some processes and procedures that will align ITAM, EUC, and ServiceDesk to deliver great service for your users.

1. Provide front-line teams with Inventory data

Accurate and available inventory information allows front-line IT teams to close requests & resolve incidents more quickly. It enables them to immediately identify which machines are in use by which users and when. Inventory data provides them with critical software deployment data such as OS version and patch level, and which applications are installed on a given machine.

This information can cut hours from a Service Request. Knowing what's installed and in use provides an install list for EUC. And hardware information may enable ServiceDesk to discover a certain machine type is generating a Known Error.

2. Make license compliance the responsibility of EUC & Service Desk

This will be a controversial request, but a necessary one. Work with your senior management to develop policy statements that make the front-line teams responsible for ensuring that only software for which you own licenses is installed. Put appropriate policies in place regarding Shadow IT. Individual agents and engineers must be responsible for this otherwise license compliance checks may be skipped when SLA deadlines loom. Remember license non-compliance is often generated when the application is first installed, not first used, and this policy protects your organisation from that. Similarly, for SaaS, you're ensuring that sensitive data is protected by only using services that have been vetted by your compliance teams. You're closing the stable door before the horse has bolted.

3. Provide accurate and timely license availability data

In order to make license compliance the responsibility of front-line teams you have to ensure that timely & accurate license availability data is available. Manually reviewing IT Requests for software license compliance is a tedious and time-consuming activity and often error prone. If ITAM becomes a bottleneck, it will be bypassed or blamed for getting in the way of delivering excellent customer service and achieving organizational objectives such as providing the right tools for employees to do their jobs.

4. Incentivise front-line teams to optimise software deployments

Laptop rebuilds and upgrades are common tasks for EUC Teams, and often more time-consuming than issuing a brand-new device. User settings and data need to transferred, along with any application customisations. To ensure software deployments are optimised it is important to ensure that only previously-used software is re-installed. Not only does this prevent license wastage it also cuts the build time for the EUC team.

To enable this, provide your EUC teams with access to usage data. This enables engineers to determine whether an application is in use. This is a great way of getting back those unused Adobe, AutoCAD, Visio, and Project licenses – all software applications notorious for being under-utilised.

Furthermore, incentivise your front-line colleagues by reporting on the value of unused software that they recover. Those colleagues rarely get the opportunity to demonstrate they're saving the organisation money and even a few thousand dollars of recovered software per month is worth celebrating. This is a great way of building rapport and demonstrating that ITAM can drive service delivery and cost-savings side-by-side.

5. Keep accurate records to streamline deployment of non-standard software

Much of your software may be covered by volume license agreements with shared license/activation keys. However, for non-standard applications that are licensed individually, it is vital you keep a record of serial numbers, product keys, named users, and install media. You also need to ensure that license keys have been recovered from old machines prior to reactivation on the new machine. You need to provide serial numbers and other information to the EUC team in an easily-accessible but secure form. Once again, there are opportunities for automation here.

Failure to keep accurate records slows down the build process and frustrates end users who need specialist software to do their job. You don't want to lock your Senior Designer out of AutoCAD for a minute longer than is necessary. The people in the firing line are your front-line teams – you owe it to them to provide accurate data in a timely fashion to serve their customers as efficiently as possible.

6. Building an automated service delivery framework

Much of this stakeholder analysis has focused on practical aspects of day-to-day interactions between people in Service Desk, EUC, and ITAM teams. These human interactions are vital when you're working to optimise the fulfilment service being provided to your customers. You will deliver service improvements by following them, but ultimately you will hit a barrier caused by the sheer scale and cadence of the tasks at hand. This is where automation plays a role, and where having a close stakeholder relationship with your front-line teams will really accelerate your ability to deliver world-class ITAM & EUC services.

So, what does automation look like? Well, it began with software deployment tooling enabling the packaging and management of common applications – tools such as SCCM have been in place to deliver this for many years. Where next-generation automation comes to the fore is in building compliance checks and service enhancements around those tools. One such approach is Enterprise App Stores.

Enterprise App Stores

Enterprise App Stores provide end-users with the ability to request their own software without any involvement from Service Desk or EUC. Requests can be pushed into a workflow whereby their line manager authorises the request and a check is made to ensure licenses are available – thereby ensuring license compliance. Once authorised the software is installed automatically.

App Stores and automation also facilitate the removal of software. Rules can be created to automatically remove unused software based on usage data gathered by your SAM tool, with jobs being automatically created in your deployment tool.

Delivering such an automation project is complex and depending on the buy-in your ITAM team has, may be challenging to deliver alone. By enlisting the support of your front-line teams, you can begin to build critical mass behind the project and make it about customer service rather than compliance. Service is often a more compelling motivation for senior leaders, particularly with an increasing focus on improving employee experience.

Summary – ServiceDesk & EUC stakeholder engagement

Front-line teams, users, and ITAM teams share a number of common goals. By identifying these shared goals – such as timely delivery of the right laptop with the right licensed software – you can work with those teams to develop processes and tools to improve user satisfaction. And you can do that whilst ensuring license compliance is not impacted and even potentially reduce software usage across your estate.

Having examined this key stakeholder relationship, the next section explores how engagement with your IT Security team can be foundational to effective IT Management – and also elevate the importance of your ITAM practice.

ITAM & IT Security

IT Security is constantly in the news. High-profile cyber-attacks such as those that befell Maersk & Equifax have had a huge impact. Maersk had **limited IT capability for two weeks** [8] following the NotPetya worldwide attack. **A vulnerability in open source software** [9] resulted in C-Suite retirements at Equifax and those same executives having to explain themselves to Congress. The breach impacted over 145 million customers worldwide and to date Equifax has spent **$1.35bn on remediation** [10] and set aside a further $800m for fines and compensation. To put that in perspective, that's equivalent to their total three-year net income from 2015 to 2018. All because of what Congress saw as an **"entirely preventable"** [11] attack.

Unsurprisingly, this means that cyber security, alongside privacy, is very high on the C-Suite priority list – and no longer something for just your CIO or CISO (Chief Information Security Officer) to worry about.

IT Asset Managers & IT Security professionals are "fellow travellers" with many of the same challenges and opportunities. By working together, each can deliver their own programmes whilst radically improving the safety and manageability of their IT estates.

Common Ground

How do IT Security & ITAM responsibilities and motivations overlap? In this section we'll explore three key commonalities – Discovery & Inventory, Risk Management, & Audit-Readiness.

Discovery & Inventory

The introduction to the recent **NIST reference framework** [12] for an IT Asset Management system states:

"IT asset management (ITAM) is foundational to an effective cybersecurity strategy and is prominently featured in the SANS Critical Security Controls and NIST Framework for Improving Critical Infrastructure Cybersecurity"

(Sidenote: NIST is the US National Institute of Standards & Technology with a wide-ranging remit including standards for US commercial & governmental computing. The NIST **Framework for Critical Infrastructure Cybersecurity** [13] is a reference framework implemented by many IT Security teams worldwide.)

Why is ITAM foundational to an IT Security programme?

The starting point comes from the cybersecurity mantra "you can't secure what you don't know about". This is what brought Equifax to its knees – firstly not everyone received the notification regarding the vulnerability, and secondly network intrusion detection systems were misconfigured. For more on this see Rich Gibbons' deep dive into the ITAM perspective on the **Equifax breach**[9].

This should sound familiar to ITAM managers – accurate and comprehensive discovery and inventory data is also foundational to our activities. Without accurate data we can't make informed decisions on future license purchases, or we may have previously unknown non-compliance positions uncovered in a software license audit.

Risk Management

It isn't just about discovery and inventory though; ITAM & Security have much more in common. Both functions seek to protect their organisations from risk, even if the risks they manage differ. Whilst ITAM focus broadly on long-term financial risks surrounding the use of IT assets, IT Security is working more in the here-and-now to defend against the daily risk of cyber-attack. However, you'll still find a common vocabulary and approach if you speak to your IT Security team about risk management. You will find many partnership opportunities are presented in contributing to and managing your organisation's Risk Register.

Audit-Readiness

Both functions also work with an expectation of being subjected to audit. For IT Security, much effort is expended on ensuring an organisation is compliant with requirements such as Sarbanes-Oxley (SOX), the Payment Card Industry PCI-DSS requirements, and other regulations such as HIPAA. These are annual audit requirements for many organisations. That's before we get to the privacy requirements of the GDPR and upcoming privacy regulations such as the California Consumer Privacy Act (CCPA). For ITAM, the audit risk is external and primarily from software publishers.

This results in both teams operating from a state of preparedness – ready for that next large-scale cyber-attack, a software license audit from a publisher, or internal or external audit. Getting to that level of readiness can, and should be, a shared journey. ITAM is essential to audit readiness for PCI-DSS because companies processing payment cards must have full hardware, software, and user visibility of their CDE (Card Data Environment).

Practical Stakeholder Engagement with IT Security

Having identified this common ground, how do we go about building a strong relationship with our IT Security teams? There are a number of practical approaches that will ensure that ITAM & IT Security motivations and objectives are aligned.

1. Discovery & Inventory

Discovery and Inventory is challenging for both teams. Getting a full picture of an estate takes time and can be a constant battle, particularly for ITAM teams who may not have the leverage to collect ITAM information on every device throughout the estate. For this reason, a common approach to this challenge is worth exploring.

The NIST framework recommends that a single version of the truth – a central asset register – is populated from multiple sources of asset data. With the right normalisation and reconciliation activity it becomes possible to build a rich, multi-faceted view of an asset throughout its lifecycle. This has the potential to eliminate blind-spots and provide certainty about your assets.

Whilst each team may require a different view of an asset – for example, an ITAM team will be interested in the precise SKU for software, whereas IT Security might just be focused on its patch level – a single, centralised asset register can provide that. If you're struggling as an ITAM manager to get your ITAM-specific agents deployed across your network – particularly in sensitive areas such as Industrial Controls or your CDE – your IT Security team might have a stronger mandate to make that happen. Everyone then benefits from that single, golden, version of the truth. This asset register is available to other IT Management disciplines such as Incident, Change and Configuration Management, and so on.

2. Incident Response

Cyber-attacks are a fact of life – it's not a case of if, but when. Data gathered by multiple toolsets can precisely identify which assets are vulnerable and susceptible to attack by referencing threat databases such as the **National Vulnerability Database – NVD** [15]. In turn, this can inform your company's mitigation strategy for those devices – do you turn them off, can you patch them, etc. The ITAM team may be the only repository of information as to the support status of an asset or software application. With the growth in hardware/firmware vulnerabilities such as **Meltdown and Spectre**, [16] information regarding the physical properties and warranty status of an asset has become important to IT Security teams. Once again, this is information that ITAM teams routinely collect and manage.

3. Lifecycle Management

So far, we have focused on the here-and-now aspects of ITAM & IT Security co-operation. However, there are also areas of long-term, strategic collaboration to explore. One such area is software lifecycle management.

Historically, perpetually-licensed software saw a pattern of major releases being granted long-term support rights. For example, Microsoft's standard support lifecycle was "5 plus 5" – 5 years of mainstream support followed by 5 years of security updates. Knowing the maturity of your software assets in relation to the software lifecycle is vital. For example, if you're running Windows 7, it is important to know that extended support for that OS ends in January 2020. This directly impacts the compliance status of environments.

4. Support contract optimisation

Software Support is no longer just about being able to call someone because something has broken, or as a way of enabling entitlement to new releases. More critical is that the support status of your software estate is critical to IT Security. Standards such as PCI-DSS mandate that software running in your CDE is still in support, and that you have an active support contract in place. This immediately makes lifecycle management a shared responsibility between ITAM & IT Security. From an ITAM perspective you can enlist IT Security requirements around this to bolster discussions on software maintenance renewals. In turn, particularly for mature or legacy software, this may help you address potential license non-compliances or to modernise your estate.

Building for the future

The IT security threat landscape and **attack surface** [17] is changing and changing rapidly. Two areas of potential co-operation to address this will be Internet-of-Things (IoT) & Third-Party Risk Management.

Internet of Things Management

Software is becoming ever closer to customers as IoT devices proliferate. We've already seen **issues raised** [18] around privacy and security of automotive systems. This presents questions around who is responsible for patching the software in company products. Will the automotive industry see safety recalls due to faulty software? Are companies responsible for keeping an inventory of the software and hardware devices they've sold? Does that responsibility extend to a smart toothbrush that connects to a company database via Bluetooth? These are the sorts of questions that keep IT Security professionals awake at night, and ones that ITAM can answer for them.

Managing Third Party Risk

A number of recent high-profile security breaches have been traced to vulnerabilities in third party service providers. For example, **Ticketmaster** [19] was breached because third-party code providing live chat functionality to their payment page was compromised. A similar vulnerability was exploited at **British Airways** [20], resulting in a proposed $225m fine. These breaches highlight the importance of discovering and inventorying all software, regardless of the source, running in your environment. This can be a joint effort between ITAM & IT Security – for example by analysing open source software running on your network and determining its quality. Very much an emerging area of collaboration that will in time improve the security of an organisation's software estate.

Engagement with IT Security – Summary

IT Security & IT Asset Management can work together to deliver shared goals. Building a shared, rich, single version of the truth about the IT infrastructure enables the organisation to maintain audit-readiness, manage risk, and ensure compliance with regulatory and legal requirements. These goals increasingly protect customers and products from threats, putting IT Security & Asset Management at the forefront of value creation and delivery for the organisation.

With front-line IT staff engaged in your ITAM practice, and IT Security benefitting from your data and insight, the final key stakeholders to elevate ITAM to the strategic stage are Business Analysts & IT Architects.

ITAM for Business Analysts & IT Architects

Where IT Security & EUC are primarily focused on the here and now, Business Analysts & IT Architects are strategic visionaries. Working with them supports strategic ITAM activities – supporting value creation, digital transformation, and delivering on long-term business goals.

What do they do?

IT Business Analysts (BAs) work with business stakeholders to find, select, and agree on solutions to business requirements. For example, a business stakeholder will engage a BA to determine the best way to improve the service delivered by a customer contact centre.

Technology Architects take the output from the BA process and design a solution to deliver the desired outcomes for the business stakeholder. Alongside this, they also take a high-level view of the IT capability of the organisation as a whole, recommending, specifying, and designing infrastructure-wide enhancements. The aim is to understand the "as-is" technology landscape and interdependencies & provide the organisation with the IT architecture that meets their current and future needs.

Common Behaviours

Strategic View

Both roles work strategically and have a broad view of the organisation's technology landscape. BAs may specialise in certain areas – for example, workflow & collaboration solutions – and similarly there are both generalist and specialist architects. For example, Cloud Architects are critical to digital transformation programmes as organisations move workloads from on-premise to cloud.

Managing Technical Debt

Whilst they are looking ahead, they also need to focus on managing the existing technology portfolio – understanding whether existing assets can be leveraged to deliver new capabilities or determining when applications and services are reaching end of life. They'll understand if there is an element of the technology portfolio that's getting in the way of the business delivering value for its customers and recommend solutions.

Managing Uncertainty

Both roles work to manage uncertainty for an organisation. They are bringing order to a degree of chaos – distilling a desired business outcome into a robust, serviceable, cost-effective solution that's fit for purpose. These are first and foremost creative roles, enabling efficient decision-making and predictable, cost-effective IT delivery against an agreed business case.

What is ITAM's role?

The nature of IT means that there are many ways to achieve a desired business outcome.

Architects and BAs have to decide whether to build a solution in-house, or to buy an application or service. They need to decide where the solution will be deployed – on premises, or in the cloud - and they need to know how the solution will be managed once deployed.

Before all that though, they need to gain insight into what the current application & service portfolio looks like. This task is not be underestimated. An organisation's IT landscape evolves over many years and mapping technology assets to products and services is complex, particularly without robust ITAM & IT Service Management. Without this, discovery is reliant upon documentation or individual knowledge.

Without certainty about your environment it becomes easy to cause unintended disruption by making a change to a system that you don't know other systems are relying on. Understanding relationships between systems also enables strategic decision-making. The first deliverable therefore is to provide Architects and BAs with a normalised, high level view of the technology assets in use, and **their interdependencies** [21].

With interdependencies mapped and discovered it becomes possible to answer questions such as "Where should I target technology investments in order to receive the greatest benefit?" For example, by mapping interdependencies, you may identify that a back-office system is a key shared component of several products and services and is therefore a prime candidate for upgrade, or that it needs to be covered by an enhanced Service Level Agreement. By leveraging inventory & discovery data ITAM can improve this key activity carried out by architects & BAs.

Leveraging Inventory & Discovery Data

This activity bridges ITAM data, the CMDB, and Application & Service Catalogues. The key information that ITAM contributes here is what is installed (and available), support status, cost, usage, and manageability of a given asset. For example, ITAM will know the upgrade/downgrade rights for a software title. ITAM will also know where that application is in its lifecycle – is it in mainstream support, extended support, or **end of life** [22]. With this information, BAs and Architects are able to identify the best use of existing technology assets. If they know that a product is going to be out of support in two years, they can plan accordingly – for example by making a strategic decision to replace that product with a more up-to-date version which may offer increased functionality.

Solution Decision Support

With clear view of the existing landscape, along with a technology strategy roadmap, ITAM's next deliverable for Architecture & Business Analysis is to help assess the various options for delivering a new application or service. Typically, for ITAM, this will focus on ensuring that any investments are cost-effective. The detailed knowledge ITAM professionals hold about the organisation's environment enables them to model various deployment and asset acquisition options. Business Analysts in particular may be assessing 3 or 4 options for meeting a requirement. ITAM professionals are uniquely placed in the organisation to provide accurate cost estimates. A strategic ITAM team models the **TCO, NPV, IRR, or other financial metrics** [22] of potential technology investments.

Enabling Digital Transformation

ITAM teams are a key stakeholder for digital transformation programmes for three reasons.

1. They have the entitlement and deployment data necessary to ensure a transformation programme doesn't add license compliance risks.

Consider the scenario of a Datacentre Architect seeking to add capacity to an on-premises Datacentre, or to shift workloads to public cloud. Adding capacity on-premises will increase license demand and the ITAM team will be able to advise the best approach to meeting that demand, thereby ensuring license compliance. For the cloud deployment scenario, an ITAM team may determine that existing on-premises license entitlements can be used to reduce cloud costs. They may also be able to reassign licenses freed up by the cloud shift to improve in-house capability. Furthermore, in European Union countries, they may be able to dispose of those redundant licenses in the **secondary software market** [23], reducing the total cost of the project.

2. ITAM Teams have licensing knowledge essential to enterprise-wide transformation programmes.

The holistic view ITAM teams share with Architects means that by working together they can transform the organisation's technology capability. Building the business case and funding for transforming a company's underlying architecture and capability requires a multi-disciplinary approach well-suited to ITAM teams.
BAs & Architects will focus on technical capabilities and outcomes and ITAM teams will model the TCO using licensing and environment knowledge. For example, the ITAM team may advise that the most cost-effective approach to improving database capabilities is to create a dedicated cluster for Oracle Database or SQL Server. Or, they may recommend that making a long-term commitment to a database technology in the form of an Oracle ULA (Unlimited License Agreement) or Microsoft SCE (Server & Cloud Enrolment) is the way to go.

3. ITAM Teams are able to help Architects & BAs identify areas for rationalisation or standardisation, or where under-used capabilities may be leveraged to improve service.

An example I encountered was a long-standing unlimited deployment entitlement for what had been earmarked as legacy software. It became possible to use this entitlement to fulfil a new demand for the capability it provided, resulting in a 6-figure cost reduction for the project. This was made possible by ensuring that the ITAM team was consulted during the business analysis and architecture phases of the project delivery. In the case of application rationalisation, the ITAM team will have the rich application and usage data to answer questions such as "Which productivity applications are under-utilised?" or "Which design package should we standardise on?"

Engaging Business Analysts & Architects

This whitepaper has outlined how strategic ITAM can improve the decisions made by Business Analysts and Architects. Whilst much of your engagement as an ITAM manager with these functions will be ad hoc, there are also practical opportunities to formalise your relationship with them.

1. Ensure Process Engagement

The first opportunity is to ensure that ITAM is consulted as part of the BA & Architecture process. Both functions will have processes in place for managing requests; ensure that ITAM sign-off is mandatory for all requests. Find out how your organisation selects & delivers new solutions and determine where an ITAM checkpoint is required. Ideally, there will be several checkpoints that involve automated workflows between **Demand Management** [24] and ITAM in order to ensure projects don't get to the delivery stage without well-defined hardware and software specifications. You don't want to be giving the project manager the bad news that a license requirement has been missed and as a result the project will require unbudgeted funding. By placing checkpoints, you ensure that any such issues are uncovered early enough that remediation can take place without it affecting delivery.

2. Work with your Programme or Project Office

Your next opportunity is to work with your Programme or Project Office to gain an overview of all initiatives with a hardware or software component. This overview, coupled with your own holistic view of the IT landscape, will enable strategic decision-making and identification of synergies. For example, this will enable the ITAM team to forecast demand, which in turn influences conversations with procurement and vendors.

3. Communicate Regularly

Set up regular meetings with your Architects and Business Analysts. Given the wealth of information the ITAM team possess, they will welcome the ITAM team to the decision-making table. The aim is to understand their motivations, areas of research, and high-level deliverables, and to map those to your knowledge of the IT landscape. ITAM enables Architects and Business Analysts to mitigate risk to their projects up front, thereby increasing the success probability of the project. If your organisation is struggling to solve technical debt, presenting a common view or solution will help gain C-Suite buy-in to resolve those issues.

Summary

Working with Business Analysts & Architects enables ITAM teams to help improve the technology capability of their organisations, whilst also meeting their objectives around cost reduction and risk management. Strong relationships with these stakeholders elevates ITAM to the level of strategic technology partner as we enable companies to make well-informed decisions on their technology investments.

Conclusion

This whitepaper has demonstrated how ITAM can build relationships by providing value to frontline IT, Security, and Architects and Business Analysts. These strong relationships place ITAM at the centre of IT Management and Governance.

These relationships are further strengthened by technology.

A CMDB provides a single, golden view of the technology landscape.

Automation enables optimisation at scale.

Enterprise App Stores improve customer service.

And decision support sytems leverage all of this to enable decision-makers to make fully informed, accurate, and optimised decisions. At the centre of all this is ITAM, equipping the organisation for a future where IT is embedded in the value chain, closer than ever to its customers.

About ServiceNow

ServiceNow (NYSE: NOW) is the fastest-growing enterprise cloud software company in the world above $1 billion. Founded in 2004 with the goal of making work easier for people, ServiceNow is making the world of work, work better for people. Our cloud-based platform and solutions deliver digital workflows that create great experiences and unlock productivity to approximately 5,400 enterprise customers worldwide, including almost 75% of the Fortune 500. For more information, visit **www.servicenow.com**.

About The ITAM Review

The ITAM Review began in 2008 so that anyone involved in the SAM or ITAM industry could share their expertise, feedback and opinions of the technology and services in the market for the benefit of others. Our mission is to provide independent industry news, reviews, resources and networking opportunities to Vendors, Partners, Consultants and End Users working in the areas of ITAM, SAM, and Software Licensing

Author Biographies

AJ Witt, Industry Analyst, The ITAM Review

AJ Witt is an experienced IT Asset Manager with a 25-year career in FTSE100 & Fortune 500 companies. At The ITAM Review he specialises in SaaS Management & Tooling.
A graduate of the School of Management & Finance, University of Nottingham, he enjoys music, travel, cycling, and spending time with his family.

Bibliography

[1] The ITAM Review, "User Survey 2018," [Online]. Available: https://www.itassetmanagement.net/2018/11/07/decade/.

[2] ServiceNow, "How ServiceNow ITBM supports IT Value Process Best Practice," [Online]. Available: https://www.servicenow.com/lpwbr/how-servicenow-itbm-supports-it-value-process-best-practices-as-defined-by-it4it.html.

[3] Wikipedia, "My Friend Cayla," [Online]. Available: https://en.wikipedia.org/wiki/My_Friend_Cayla. [Accessed 30th July 2019].

[4] The Independent, "TSB IT Failure," [Online]. Available: https://www.independent.co.uk/news/business/news/tsb-it-failure-cost-compensation-customers-switch-current-account-a8757821.html. [Accessed 30 July 2019].

[5] R. Gibbons, "Equifax and Cybersecurity," The ITAM Review, [Online]. Available: https://www.itassetmanagement.net/2019/02/15/equifax-and-cybersecurity-a-deep-dive/. [Accessed 30 July 2019].

[6] ServiceNow, "Weaponizing SAM," [Online]. Available: https://workflow.servicenow.com/it-transformation/weaponizing-sam/. [Accessed 30 July 2019].

[7] A. Witt, "NIST Cyber Security Guide for ITAM," [Online]. Available: https://www.itassetmanagement.net/2018/11/15/nist-cyber-security-guide-for-itam/. [Accessed 30 July 2019].

[8] A. Witt, "Authorised Software Install costs Maersk $300m," The ITAM Review, [Online]. Available: https://www.itassetmanagement.net/2018/08/31/authorised-software-install-costs-maersk-300m/. [Accessed 30 July 2019].

[9] R. Gibbons, "Equifax and Cybersecurity - a deep dive," [Online]. Available: https://www.itassetmanagement.net/2019/02/15/equifax-and-cybersecurity-a-deep-dive/. [Accessed 30 July 2019].

[10] SC Magazine, "Equifax Data Breach Recovery Costs pass $1bn," [Online]. Available: https://www.scmagazine.com/home/security-news/data-breach/equifax-data-breach-recovery-costs-pass-1-billion/. [Accessed 30 July 2019].

[11] GovTech.com, [Online]. Available: https://www.govtech.com/security/Congressional-Report-Equifax-Breach-Entirely-Preventable.html. [Accessed 30 July 2019].

[12] NCCOE, "1800-5 Volume B," [Online]. Available: https://www.nccoe.nist.gov/publication/1800-5/VolB/index.html. [Accessed 30 July 2019].

Bibliography (cont.)

[13] Wikipedia, "NIST Cybersecurity Framework," [Online]. Available: https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework. [Accessed 30 July 2019].

[14] NIST, "NVD," [Online]. Available: https://nvd.nist.gov/. [Accessed 30 July 2019].

[15] Meltdown Attack, "Meltdown Attack," [Online]. Available: https://meltdownattack.com/. [Accessed 30 July 2019].

[16] Wikipedia, "Attack Surface," [Online]. Available: https://en.wikipedia.org/wiki/Attack_surface. [Accessed 30 July 2019].

[17] T. Hunt, "Controlling vehicle features of Nissan LEAFs across the globe via vulnerable APIs," [Online]. Available: https://www.troyhunt.com/controlling-vehicle-features-of-nissan/. [Accessed 30 July 2019].

[18] The Register, "Ticketmaster denies fault with website led to Magecart infection," [Online]. Available: https://www.theregister.co.uk/2018/12/12/ticketmaster_denies_fault_website_magecart_infection/. [Accessed 30 July 2019].

[19] Computer Weekly, "British Airways Data Breach worse than thought," [Online]. Available: https://www.computerweekly.com/news/252451391/British-Airways-data-breach-worse-than-thought. [Accessed 30 July 2019].

[20] ServiceNow, "APM | The Big Picture," [Online]. Available: https://www.youtube.com/watch?v=Du4ae9B6ans&list=PLCOmiTb5WX3o2ZlBuZqlJiDZ_Hz4l3zJv&index=3. [Accessed 30 July 2019].

[21] ServiceNow, "APM | Overview," [Online]. Available: https://youtu.be/uMK-2C4fpeg?t=192. [Accessed 30 July 2019].

[22] A. Witt, "Secondary Software Market Guide," [Online]. Available: https://www.itassetmanagement.net/marketplace/topic/market-guides/secondary-software-market-guide. [Accessed 30 July 2019].

[23] ServiceNow, "IT Business Management," [Online]. Available: https://www.servicenow.com/products/business-management.html. [Accessed 30 July 2019].

[24] Wikipedia, "Zero-day (computing)," [Online]. Available: https://en.wikipedia.org/wiki/Zero-day_(computing). [Accessed 30 July 2019].