Become a partner in protection

AXIS COMMUNICATIONS

Forward

Cybercrime is surging at an exponential rate, and the threat it poses to businesses today is real and present. Businesses depend on their technology, with digital systems that are their organization's very backbone. But while these systems are essential to an organization's prosperity, if breached by cybercriminals, they can also cause its downfall. There's even a phrase for it: 'Cyber Fatality', meaning a digital breach so severe that it puts a company out of business. Protecting critical company data, such as customer, financial and operational data, as well as intellectual property, is now one of the most important issues facing business leaders today.

Securing data has also become political with the introduction of the General Data Protection Regulation (GDPR) in the EU, and an assortment of state and federal rules in the US, all geared to safeguard customer and company data. However, while organizations are committed to finding ways to increase data protection, cyber criminals are committed to finding ways to beat them. Moreover, companies who neglect to address their data protection responsibilities, and fall victim to cyberattacks, are now facing the threat of huge fines, loss of customers and damage to their reputation. It's therefore safe to say that faulty cybersecurity and data breaches have emerged as the one of the biggest threats to business leaders today.

But what about system integrators? What part do you, as a supplier, play in the war on cyber criminals and data breaches? And what, if any, are the business opportunities therein?

Adequate protection

In the EU, GDPR was put in place to give people greater control of their personal data and to create a uniform level of data protection across the EU, fitting for the digital age we live in. Hence, organizations now have the responsibility to ensure that their customer data is adequately protected from cyberattacks and data breaches. Failing to do so can have dire consequences. Governments and regulators, such as the Information Commissioner's Office (ICO), are coming down hard on companies not adhering to the strict regulations, meting out hefty fines of up to 4% of an organization's global turnover or €20m – whichever is higher. Both British Airways and Marriott International, for example, made headlines in 2019 for huge fines incurred for losing customer data following a cyberattack.

The US is also cracking down on how companies collect and handle personal data. And while there is no federal GDPR equivalent, there are state and federal rules governing data protection. The California Consumer Privacy Act of 2018, for example, is similar to the EU's GDPR and companies that hold data on more than 50,000 people must comply or face fines.

> **"Organizations now have the responsibility to ensure that their customer data is adequately protected**

The threat of non-compliance

The threat of fines and penalties has clearly sent shockwaves through the business community. Research by data security company Clearswift shows that the threat of fines is now having the greatest impact on UK cyber security spend. Clearswift also reports that 32% of companies reference the British Airways and Marriott International cases as the primary reason for an increase in board level involvement and/or provision for their IT security spending.

> **“ Cyber criminals are becoming more and more sophisticated in their approach**

The risk of heavy fines for non-compliance is not the only concern for companies addressing cybersecurity. Organizations are also under threat of other targeted attacks, such as ransomware, malware, and phishing. Cybercriminals are becoming more and more sophisticated in their approach and are relentless when looking for new ways to penetrate IT systems. Defenceless companies face fines, system shutdowns, lost data, operations paralysis, bad press, loss of customers and revenue dips. Is it any wonder that organizations, from the Chairperson of the Board to the IT support staffer, are sitting up and taking notice?

From supplier to trusted partner

Companies therefore need to be wise in their selection of IT systems, their service and maintenance agreements and, above all, their choice of system integrator. They need a system integrator/supplier who understands today's cyber landscape and its threats, and who can demonstrate considerable cybersecurity integrity and maturity. Simply put, cybersecurity takes more than just products with cutting-edge technology. It's also about ongoing processes that require effort, knowledge and experience to maintain.

By choosing to offer customers support to address their cybersecurity risks, and a hardware management strategy, you can become a trusted long-term partner, and not just a supplier.

> **"Simply put, cybersecurity takes more than just products with cutting-edge technology**

A trusted long-term partner

By offering support addressing cybersecurity, you open the door to new opportunities, for you and your business. You can build customer confidence and loyalty by demonstrating that your offering goes beyond generic service and maintenance agreements to cover cybersecurity support and a hardware lifecycle management strategy. In short, you become a stable partner, protecting your clients and helping them mitigate the risks of cyberattacks. You're also future proofing your own business by creating long-term opportunities, rather than short-term gigs.

Grow your business

Here at Axis, we have seen that system integrators exhibiting this kind of cyber maturity are significantly more likely to win new contracts. What's more, integrators who understand the challenges companies are facing when it comes to cybersecurity, and who can demonstrate their cyber maturity, also gain greater trust from their existing customers. It's a win-win situation, where you can align your offering to alleviate some of the risks associated with cyberattacks through physical security systems, sow the seeds for new opportunities, and grow your business.

Not just a supplier

Experience has shown that the role of the IT department in organizations is becoming more influential and that IT managers now have a significant impact on the decision-making process, and on whether or not to acquire costly additional services. We know too that more and more IT decisions-makers and security departments now expect contractors to update systems, patch firmware and advise on security issues. In a nutshell, they are looking for a partner, not just a supplier.

Become a trusted partner and:

- Increase customer satisfaction
- Drive customer loyalty
- Win more contracts
- Grow your business

The value of the service and maintenance contract

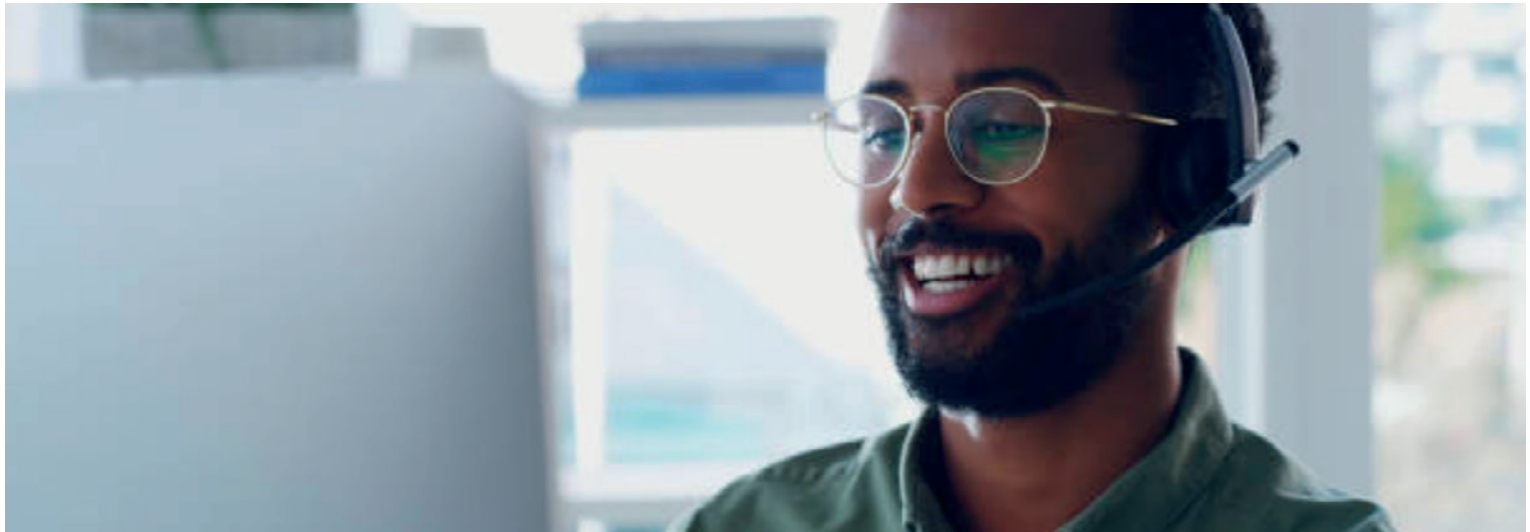
While some systems integrators may have seen service and maintenance contracts drop in recent years, this certainly hasn't been the case for those charged with maintaining IT systems. What is noteworthy here, is that physical and electronic security systems now largely use the same infrastructure as in-house IT systems. Consider the impact of this, and whether or not it changes the value of a service and maintenance contract?

Beyond the warranty

In the past, a traditional planned preventative maintenance contract would have covered both the physical and electronic security system installations. The contract would stipulate regular inspections to see if all cameras were still connected to the system, if image quality were still optimized and, often, a device inspection onsite. Those days are long gone. So, is it any wonder that we have seen a reduction in the number of service and maintenance contracts being issued beyond the warranty and defects period from some clients?

Regular updates and security

But if there is no service and maintenance contract in place, who then is responsible for maintaining the cybersecurity integrity related to these systems? And who is making sure that regular updates are being carried out, and that system security is maintained?



The value of the service and maintenance contract, continued

Consider this

If you have been appointed as the customer's service and maintenance provider, then the expectation is that this covers all aspects of both the hardware and the software, unless contractually qualified out. When negotiating service and maintenance offerings with a focus on firmware updates and patches with your client, you should therefore take the following into consideration:

1) If the client chooses to qualify this element out of your offering, ask him/her who will then be responsible for this work when the need arises. Point out the potentially negative knock-on effects of another stakeholder carrying out work on a system that you have been employed to maintain.

2) If you, on the other hand, choose to qualify this element out of your offering, then think about how this will be perceived by the client, especially if your competitors are providing firmware updates, patches and other cyber security services.

3) Being informed about cyber security will help position you favorably compared to your competitors. By understanding the manufacturer's approach to firmware updates/patches, etc. and appearing knowledgeable about the update and patching, you are showing your customers that you have the potential to be their trusted cybersecurity partner, rather than just a supplier.

Adopting an approach that demonstrates to your customers that you understand the importance of service and maintenance contacts beyond traditional planned preventative maintenance, instills confidence in the customer and supports contract wins.

The importance of firmware and patches

A disciplined approach to firmware updates and patch management is critical for good cybersecurity hygiene but can be challenging for many organizations. While the vast majority of businesses understand the necessity of keeping their operating systems and applications patched and up to date, the same does not always apply to the firmware their system hardware rests upon. In fact, often the firmware on a device is never updated at all.

Enterprises are vulnerable

This kind of poor patch management leaves enterprises vulnerable to cyber predators and, not least, to penalties and fines from regulators. Since the implementation of GDPR, we have seen numerous cases of ransomware and malware targeting firmware and causing deep damage by disabling critical infrastructure and stealing credentials. This kind of non-compliance is a fast track to the aforementioned hefty fines. And as a system integrator, you too are potentially vulnerable.

An undeniable opportunity

With such huge risks, the need for exceptional firmware update management is non-negotiable and enterprises are realizing that it is a central element to their cybersecurity programmes. The risks are huge and, as a system integrator, you have an undeniable opportunity to support your clients in avoiding these risks. And we, as your technology partner can, in turn, support you.

Mitigate risk and win new clients

The UK's ICO and the National Cyber Security Centre have developed guidance specifically related to poor patch management, off the back of breaches that have led to monetary penalties. This guidance states, 'Failure to patch known vulnerabilities is a factor that the ICO takes into account when determining whether a breach of the seventh principle of the Data Protection Act is serious enough to warrant a civil monetary penalty.'

Poor patch management

It doesn't get any clearer than that: poor patch management practice that fails to protect consumer data can have damaging consequences for global organizations. Paradoxically, according to the ICO, '60% of breaches involved vulnerabilities for which a patch was available but not "applied". This means that the terrible fallout of cybercrime (lost customer data, large fines, damage to reputation, etc.) could have been avoided simply by applying good patch management.

A duty to your clients

But who is responsible when patch management fails? Directly, it is of course the organization in question. Indirectly however, you as the system integrator have a duty to your clients to ensure they are protected, and that their customer data is fortified against any and every breach. In the worst case scenario, third parties (such as suppliers) can be partly liable for non-compliance and therefore incur a percentage of the fine.

Win the war on cybercrime

As your technology partner, Axis can work with you to mitigate these risks with tools and services that help you and your clients win the war on cybercrime. What's more, by focusing on cybersecurity, we believe you can widen your net, with a more comprehensive and attractive offering that can help attract new customers.

> **"60% of breaches involved vulnerabilities for which a patch was available but not applied**

Stay one step ahead with Axis Device Manager

So how can we help? At Axis, we have developed Axis Device Manager (ADM), an easy and cost-effective way to manage – and secure – connected devices. It arms suppliers and system administrators with a highly effective tool to manage all major installation, security and maintenance tasks.

A wide range of features

When it comes to cybersecurity, one of the key benefits of ADM is the ability to harden all Axis devices that are attached to the network, in line with the Axis Hardening Guide. The guide follows baseline uses such as the CIS Controls - Version 6.1 (previously known as SANS Top 20 Critical Security Controls). ADM offers a wide range of cybersecurity features, such as firmware management, HTTPS certificate management, user and password management. Moreover, it enables commissioning engineers to build a device profile related to device hardening. The profile can then be saved as a configuration setting and published across remaining devices, reducing the commissioning time tenfold, while at the same time creating a layered approach. In turn, this ensures limiting a single point of failure and exposure while seamlessly hardening the system.

Address CVEs

In the light of the importance of good firmware and patch management, there is no disputing the advantages of ADM. With it, integrators can proactively monitor video surveillance systems and carry out all updates – without incurring excessive costs or impacting ongoing integrations with other systems. Running ADM will allow you to track any firmware updates that have been issued and thus address any Common Vulnerability Exposures (CVEs) in line with Axis Vulnerability Management policy.

Device Inventory / Asset Management system:

- Account and Password Policy
- Efficient installation of firmware upgrades and applications
- Apply cybersecurity controls: manage HTTPS and upload IEEE 802.1x certificates, manage accounts and passwords
- Certificate lifecycle management: manage all major installation, security and operational tasks
- Fast, easy configuration of new devices: backup and restore settings
- Suitable for sites of all sizes: single or multiple site installation

The shift from warranties to firmware

It used to be that having a hardware warranty was the be-all and end-all, with firmware updates and patches coming up second – if that. Now, updates to firmware that combat data breaches are steadily becoming more important than warranties. This isn't really surprising when you consider the fact that manufacturer hardware warranties range from 1–5 years versus a technology lifetime expectancy of between 7–10 years. And that's where the disconnect lies: an expired warranty is of little or no use when faced with a cyberattack and breach of data. Good firmware management, however, is priceless.

That's why the focus is shifting from warranties to firmware strategy and what system integrators can offer to assuage risks. Enterprises today know that just because their hardware warranty has run out, it doesn't necessarily mean that the manufacturer has stopped providing firmware patches and updates.

Active or LTS?

A case in point is the programme that Axis offers, as part of the ongoing lifecycle management of our devices. This programme gives users the choice between Active Support and Long-term Support (LTS).

In the Active track, we continuously add features, while also working on improvements to cybersecurity and stability. In the LTS track, however, we don't add new features but instead focus on stability and cybersecurity enhancements. If your device comes already loaded with the features you need, then we recommend the LTS ttrack as it addresses a fundamental concern that many enterprises have when it comes to firmware updates – the fear that firmware updates will result in a loss of some or all of the new features and integrations that have been added on. With the LTS track, this is no longer a concern as no new features are added.

Innovation drives technology

Be that as it may, nothing lasts forever; not even the best equipment. Innovation drives technological change and opportunities arise. And while operational features to address business problems have always been high on an organization's agenda, justifying these upgrades, and the costs they incur, can be tricky, especially if you don't have a potent business case. Try, instead, to shift the focus away from operational efficiency and towards cybersecurity. This will likely open more doors and is often easier to justify budget for.

End-of-life versus end-of-support

As mentioned earlier, nothing lasts forever and, as a supplier, you will most likely be called upon to assist your clients with their equipment replacement strategy. Two key factors that need to be considered are End-of-Life (EOL) and End-of-Support (EOS), and the difference between the two. Keep in mind, however, that there are opportunities to be leveraged by both.

EOL

"End-of-life" (EOL) is a term used with respect to a product supplied to customers, indicating that the product is in the end of its useful life (from the vendor's point of view), and that the vendor will stop marketing and selling it. This usually occurs when the vendor has a newer and better alternative available. This doesn't mean that organizations using this technology should panic; it often simply signals that there's a new and improved alternative available. EOL should go hand-in-hand with EOS documentation, communicating to the customer when EOL is recommended and when support will cease. Incidentally, EOL should not impact a manufacturer's warranty period.

EOS

End-of-support (EOS) denotes a situation where a manufacturer/developer ceases support for a product or service. This typically refers to both hardware and software and is something that enterprises who have technologies deployed across their organization must carefully monitor. It is essential to understand a manufacturer's EOS strategy, and how long they plan to support the hardware or software once the product has entered EOL. This information is vital to IT professionals who manage site IT policies and cybersecurity because it indicates the point at which the vendor will stop deploying updates and patches. Obviously, EOS can leave enterprises vulnerable to exploitation and data breaches.

A prime opportunity

We've established that all software and hardware will become obsolete at some point. This is inevitable, and enterprises need to take note. A recommendation from the UK National Cybersecurity Centre, is that obsolete and out-of-date software should not be used. While they acknowledge that this may not always be possible, they do highlight the likely pitfalls presented by continued use of out-of-date or obsolete software (see below).

Using obsolete software compounds two related problems:

- The software will no longer receive security updates from its developers, increasing the likelihood that exploitable vulnerabilities will become known to attackers.
- The latest security mitigations are not present in older software, increasing the impact of vulnerabilities, making exploitation more likely to succeed, and making detection of any exploitations more difficult.

High-impact security incidents

Combined, these issues mean that high-impact security incidents are more likely to occur, including malware exploiting 'wormable' vulnerabilities. Undoubtedly, the impact of such can have catastrophic ramifications across an entire organization.

A hardware replacement strategy

Of course, enterprises are not oblivious to the fact that software and hardware have a shelf life and they are therefore keen to build a hardware-replacement strategy into their annual budgets, hence allaying any unnecessary risk. This is a prime opportunity for maintenance providers and system integrators to support clients who are looking to upgrade to newer technologies. Moreover, organizations that don't have any form of lifecycle management programme in place are low-hanging fruit for security integrators, giving them the opening to proactively advise, serve and support customers. This, in turn, empowers organizations to plan ahead and allocate manpower and budget, ensuring the security and integrity of their systems remain intact.

> **"A recommendation from the UK National Cybersecurity Centre states that obsolete and out-of-date software should not be used**

The time to act is now

There is no doubt that the concerns over compliance and cybersecurity are here to stay. Enterprises and consumers are sitting up and taking notice of the threat, realizing that their systems and data are vulnerable to attack if they don't act fast. Companies want to be able to pursue innovation and growth with confidence while minimizing the many risks posed by cybercrime. And consumers want their data kept safe and private and expect the organizations they deal with to figure out how.

A competitive edge

System integrators are in a prime position to differentiate themselves by exhibiting cyber maturity and integrity. Demonstrating awareness and an acute understanding of the menace cybercriminals pose, and showing how you can underpin a company's cybersecurity strategy is a sure-fire way to set yourself apart from the competition. By the same token, are also in a great position to boost the number of service and maintenance contract wins.

A trusted advisor

The free tools that Axis provides will reinforce your offering and further safeguard your customers from the hazard posed by cyberattacks and data breaches. With these tools, you can become a trusted advisor by supporting clients with replacement strategies for EOS equipment and by enabling forward planning and long-term protection from cyber lawbreakers.

> **"Putting it simply, you become their partner in protection.**
>
> To find out more, click here.