Cryptography:
CEO Questions for CTOs

Author

Robin Wilton

Internet Technology Office

Contributors

Steve Olshansky

Ryan Polk

Andrei Robachevsky

Christine Runnegar

Jan Zorz

Internet Society

Table of Contents

Introduction

Cryptography is a complex topic – technically, operationally, and legally. As of October 2017, recent cryptography-related incidents have included Adobe publishing its private key online, the discovery of the KRACK flaw in WPA2-encrypted wi-fi sessions, and revelation of a bug in the key generation routines of Infineon processors. These failures affect millions of users and thousands of companies around the world.

- If you received an Adobe software update signed with the compromised private key, you have no guarantee that the update wasn't malicious code from a third party.
- If you use WPA2 to encrypt your home wi-fi traffic, an attacker could have been snooping on all of it.
- If your laptop uses an Infineon TPM (Trusted Platform Module) to encrypt your hard disk, that encryption may not have been providing you with the protection you expected.

These are just some examples of the risk posed by these three flaws; there are others. That said, it's not sensible to respond by excluding cryptographic tools from your enterprise. If used well, cryptographic techniques such as encryption can reduce business risk, enable business to take place securely, and protect the organisation from bad actors. If used badly, they can lead to a false sense of security, bring applications and business functions to a halt, and render data unusable.

CEOs should not necessarily be expected to understand the details, but someone has to. Businesses need to understand enough about cryptography to understand how to minimise risk, and how to mitigate the damage if they are affected.

Like any element of an enterprise infrastructure, cryptography has technical aspects, user aspects, operational and management aspects, and of course, it has to be cost-justified in terms of risk vs. benefit. Cryptography is generally used to secure sensitive, valuable assets and functions (confidential information, access control, and so on), so its failure can have particularly severe consequences. It can be complex to understand and deploy correctly, but invisible when it is working as intended. Cryptographic functions may depend on vital administrative tasks being carried out regularly but infrequently (e.g. the "rollover", or replacement, of keys and certificates that are in use). It often does not fail gracefully, so the risk of failure needs to be carefully considered and catered for.

For these reasons, cryptography is best thought of as a critical but "brittle" part of the infrastructure. It requires management and operational focus, with all the attention to planning and resources that implies - even when everything is working smoothly - so that damage and disruption are minimal if things go wrong.

How to use this document

This paper looks at the use of encryption technology under three main headings:

- Strategy and status
- Deployment and management
- Non-technical factors

Each section of this document contains a set of questions (marked with this bullet: ➢) to ask responsible executives or managers in your organisation. If the issues are clear, those may be all you need, as a reminder/checklist. However, each section describes the issues and why they are important. This additional detail may help you discuss and clarify any topics or questions that are initially unclear or unfamiliar.

A. Strategy and status

1. Is it clear why cryptography is used in our organisation?

The aim here is to be able to look at any specific use of cryptography in the organisation and relate it, systematically, to a business purpose in support of organisational goals. For example:

> "We use two-factor **authentication** [a security service], based on **one-time password tokens** [a cryptographic mechanism], for any employee **accessing corporate systems remotely** [a corporate function], to reduce the risk of **unauthorised access** to applications, data, and the IT infrastructure [risk relating to a set of identified assets]."

The ISO27000 series of standards sets out a comprehensive framework and guidance on these topics.

- ➢ Has the use of cryptographic technology in the organisation been through a review/justification process that relates it to specific business goals, benefits and risks?
- ➢ Has a vulnerability analysis been carried out, to identify risks to the organisation's assets and operations, and to identify possible technical mitigations of those risks?

2. Do we have an inventory of the use of encryption technology across our organisation?

Cryptographic technology takes many forms and can serve several purposes. An inventory will help you ensure that attention, resources, and the right technology are focused on the right areas. For example: does the organisation have a policy of using encryption in the following ways?

- ➢ Encryption for confidential communication (internal and external):
  - Session-level encryption (https, TLS), virtual private networks (VPNs)
  - Encrypted and/or digitally signed email
  - Application-level encryption (e.g. SSH)
- ➢ Encryption for confidentiality of stored information:
  - Encrypted files, disk encryption, encryption of data written to USB/removable storage
  - Archives, caches, backups, development/test copies of production databases
- ➢ Cryptography to identify people, applications and things:
  - Authentication of your corporate website
  - "Two-factor" or strong user authentication (for instance, using a hardware token)
  - Remote device authentication
- ➢ Are technical or line-of-business staff aware of any other uses? If so, what's the business rationale, and are those uses appropriately managed?

B. Deployment and management

1. Are the cryptographic services in use the right ones?

Cryptographic technology is generally used to provide two basic services: data confidentiality – (by encrypting the data), and data integrity (by using related cryptographic mechanisms to protect data against forgery or tampering). This section looks at the different forms of encryption for communicated data and stored data.

a) Data confidentiality

Communicating in confidence

The need to protect your organisation's information assets cannot be allowed to stop you from doing business: you need to communicate (internally and externally), and you need to do so without compromising the security of your data. It's vital to know whether data confidentiality services are providing the protection you expect. Otherwise, the protection you *think* you have may not match up to your risk analysis. Here are some different kinds of encrypted communication, to illustrate what protection the encryption does or does not provide:

- Session-level encryption (such as the https session between your browser and a website) means the data on the website is in clear (that is, unencrypted), and it appears in clear in your browser, but for anyone listening in between those two points, the content would only be visible in encrypted form.
- Network traffic, particularly in the corporate context, can also be secured by the use of virtual private networks (VPNs). These provide confidentiality between two endpoints, but not beyond them.
- When webmail travels over session-level encryption, the same principle applies: the email is in clear as you type it in, and it is stored in clear at the web server, but anyone intercepting it between your browser and the web server will only see the content in its encrypted form.

Note one caveat: these examples carefully referred to a third party only seeing the *content* of your communication in encrypted form. There are some things they will see in clear, even if you encrypt the content: which website you visited; who your email was sent to; the IP addresses of both parties; the date and time of the exchange; certificates identifying the server (and the client, if used), and so on. These in-clear pieces of information are referred to as "metadata". They can, in themselves, be highly revealing about who is talking to whom, or accessing which online information.

So, the kinds of encryption described above amount to a simple encrypted pipe between two points (such as a browser and a web server). They protect against interception of content, but not of metadata.

Session-level encryption can introduce a challenge for your organisation if you rely on access to the contents of network traffic in order (for example) to detect malware or the potential leakage of sensitive information. If network traffic is encrypted, inspecting its contents becomes more complicated. One option is to terminate incoming encrypted sessions at a "safe zone" inside your enterprise network and inspect the contents there, before allowing them to go on their way. Other approaches and

technical options are evolving but are beyond the scope of this paper. A recent Gartner/Radware paper[1] outlines some of the challenges that can arise when trying to reconcile the two objectives of (i) keeping traffic confidential and (ii) detecting malware and data leakages.

In the case of email, if the requirement is to make sure your email cannot be read at the server, and is only readable by the recipient, you need end-to-end encryption. This implies that the mail client is capable of encrypting and decrypting and has access to the keys it will need to do each of those things. It requires more setup and management than session-level encryption, but it protects the email through more of its lifecycle (once opened, the unencrypted contents might be copied, backed up, archived and so on, possibly unintentionally). As with session-level encryption, a lot of information remains in clear in the meta-data of email traffic, even when the contents are encrypted.

An increasing number of instant messaging clients are also capable of end-to-end encryption. Compared to email clients, these are more likely to take care of generating and storing the keys they need – making that process more transparent for the user.

Generally speaking, encrypted communication uses both symmetric and public key encryption: symmetric encryption to encrypt the data itself, and public key encryption to exchange the symmetric keys under which the data is encrypted. Encrypted communication therefore relies on use of a public key infrastructure (PKI), which introduces its own requirements in terms of management and operations disciplines. PKI will almost always introduce a dependency for your organisation, on a "trust anchor" that belongs to a third party. For instance, the certificate authority that signs the public key identifying your corporate website. More detailed observations about PKI-related factors are included in Annex B.

Keeping your secrets secret

Where the organisation has to retain data and keep it secret, encryption can form an important element of "defence in depth" against attempts to access confidential data and/or sensitive information assets. Other elements of such a defence are appropriate authentication and authorisation mechanisms, a managed lifecycle of access and permissions, auditable access logs, and physical security.

However, as Bob Blakley (Global Head of Information Security for Citigroup) puts it: “encrypting stuff is easy; the hard part is managing access to the keys”. After all, locking your front door isn’t difficult – but you have to take good care of your key, who has access to it, and who else has a copy.

Securing stored data gives rise to three principal key management requirements:

1. Ensure that only the right people/applications can access encryption/decryption keys. This is particularly important as a protection against malicious action from within the organisation itself;
2. Re-encrypt data under fresh a key if the current key is compromised;
3. Integrate encryption/decryption with the rest of the data management lifecycle (archival/backup of data, redundant copies for resilience, copies of data for development/test purposes, etc.).

Even with an understanding of these three requirements, it’s still possible to get it wrong. For example, one organisation had a backup/archival process for making a backup tape of their data and shipping it to an offsite storage facility. The backup tape was encrypted, but to ensure it could be accessed, the keys

1 https://www.gartner.com/imagesrv/media-products/pdf/radware/Radware-1-2Y7FR0I.pdf

were printed onto a label which was included in the box with the tapes - rather than stored elsewhere or sent in a secure form.

You need to be aware of who else you are trusting with the keys to your encrypted data, and what that trust is based on. If you hand a third party the encrypted data and the keys, you are essentially cancelling out the technical protection that encryption provided for your data asset.

- Correct management of keys is vital, if the protection they provide is to be maintained.
- If keys are not refreshed, data is put at risk.
- If keys and/or secure devices cannot be securely replaced, the protection they provide is compromised.
- If expired keys and certificates remain in use, the organisation's assets are put at risk.

b) Data integrity

When it comes to data integrity services, it is important to know what kind of protection you need, and ensure it is matched to an identified business risk.

If you need to be able to send emails or documents and have the recipient check that it came from you and hasn't been tampered with in the meantime, then digital signature may be appropriate. The same applies to receiving emails or documents from others.

However, if your business-critical requirement is actually for a transactional audit trail, you may find that logging and database functions are the appropriate tool. In some cases, this approach can be a substitute for digital signature (for instance, Docusign offers this as a server-side service). It's also possible to combine transactional and integrity mechanisms and, for example, digitally sign the records in an audit log.

If your organisation relies on digitally-signed documents in the long term, do you have a management process for the keys used to create and verify those signatures? What would be the business impact if you were unable to verify the signatures on archived documents?

Like session-level encryption, digital signing is usually enabled by public key infrastructure (PKI), and as above, that will almost always mean your organisation has a dependency on a third-party certificate authority (CA). That third-party dependency needs appropriate contractual cover, and a plan should also be in place to deal with a failure or compromise of the third party.

c) Other services

Authentication (of users, applications, websites, devices, and other assets) relies on encryption – either in the form of a shared secret (such as a password) or in the form of a cryptographically-secured token, such as a one-time password generator. Passwords need to be securely exchanged, which generally means sending them "out of band" (the way banks send out PIN mailers for ATM cards) or sending them over a secure session. Passwords should not be stored. They should be "salted" with a random value, then hashed, and the resulting value stored.

Your authentication processes must be able to control who gets access to the keys that encrypt/decrypt data, and sign/verify documents. That means that authentication must be the precursor to robust authorization and access control, and that access requests are properly logged and audited.

Those related disciplines (authentication, authorization, access control and audit) are beyond the scope of this paper, but are mature disciplines backed up by a wealth of applicable standards and guidance.

Many cryptographic and authentication mechanisms also rely on access to a reliable source of time-stamping (for instance, to determine whether a certificate, session, or one-time-password has expired).

Questions to ask about encryption services

- Is data in motion given the appropriate level of protection – for instance, is end-to-end encryption used where session-level encryption is not sufficient?
- What is the fallback if secure communication doesn't work, or is too slow? Will users resort to insecure communication? Is this adequately managed, through technical resilience/performance and user education?
- Is there a classification process for deciding what data at rest should be encrypted? Is that process based on a business risk assessment and a vulnerability analysis?
- Can we still recover encrypted data if, for instance, the keys used to encrypt it are lost or destroyed?
- Is it possible that employees are using encryption of their own accord, and if so, is that something we ought to know about/manage?
- What would happen if we were unable to access the data encrypted by an employee?
- Do we have a password management regime that would allow us to unlock an employee's devices or log in to their applications if necessary? Do we also have a "Bring Your Own Device" (BYOD) policy, and if so, are these two things compatible?
- Do we manage passwords securely (for instance, by salting and hashing them for storage)?
- Do we take measures to check whether encrypted data has been compromised (for instance, looking for examples of it, unencrypted, out in the open)?
- Do we treat authentication and time-stamping services as critical parts of our IT infrastructure? What processes do we have for ensuring that they remain available and resilient?

Questions to ask about Public Key Infrastructure (PKI)

➢ What services do we have that depend on PKI?

- Public key certificate to secure/authenticate access to our website
- Encryption/signature of emails
- Data integrity (signing documents, transactions and audit records)
- User authentication (e.g. smart cards, X.509 certificates, US PIV cards)
- Other services…

➢ Are those services resilient if we need to change elements of the PKI at short notice - such as the CA we use, our enterprise's root keys/certificates, or the keys/certificates used by some or all of our users?

➢ What is the basis for our trust in any third party CAs we use? What contractual/liability arrangements are in place between us?

➢ Can we manage the artefacts of PKI services? Do we depend on long-term verification of signed documents, and if so, are the necessary keys managed?

➢ Are PKI-dependent IoT devices (connected objects) present in our infrastructure, and are their PKI functions adequately managed?

➢ Who manages remote PKI functions – us, or the user? What happens if we need to remove a CA from the trusted root list in all the devices used by our employees?

➢ Is there application-level use of PKI services (such as SSH), and if so, are those uses documented and manageable?

2. Operational lifecycle

Cryptographic technology is inconvenient to deploy and is often only viable as long as it remains invisible in the infrastructure (if people have to actively configure or invoke cryptographic services, that tends to be a barrier to adoption and use and can introduce a high risk of error and therefore failure).

As noted above, systems management support for cryptography is generally weak. Consequently, changes to existing deployments of cryptographic technology tend to encounter very high organisational inertia. For example, as of March 2017, over 1/5 of websites[2] were still using PKI certificates signed with the SHA-1 hashing algorithm – that's over 30 million public-facing websites, using a crypto technology that experts have been warning, since 2005, should be replaced, because it can be cracked.

Cryptographic infrastructure tends to be "brittle". That is, it doesn't fail gracefully, and once deployed, it is inflexible and hard to modify piece by piece. As a consequence, flawed or obsolete deployments sometimes remain in use far longer than they safely should.

2 https://www.venafi.com/blog/deprecation-denial-why-are-35-of-websites-still-using-sha-1

Questions to ask about lifecycle management

➢ What is the expected lifespan, in our organisation, of:

- the algorithms we use
- the key lengths we use
- the data we encrypt for transmission or storage
- the data we sign, or have signed for our use
- the devices that use encryption (whether remote or under our direct control)?

➢ Onboarding/initialisation: do we have trusted processes for issuing and initialising encryption-capable devices (smart cards, authentication tokens, encryption software)?

➢ Can we ensure that untrusted devices are not introduced to our infrastructure?

➢ Management/replacement: can devices that are in use be securely updated, patched, or replaced promptly and without disruption?

➢ Decommissioning: can keys and data on encrypted devices be recovered, and the devices wiped/decommissioned and securely disposed of when they are withdrawn from use?

➢ Do we have the right skills in the organisation, to deploy and manage encryption technology throughout its lifecycle? Are critical skills/disciplines/roles identified and planned for?

C. Non-technical factors

1. Law enforcement access

The more dependent we become on the Internet - as citizens, consumers, companies, societies and nations – the more incentive policymakers feel to exert some level of policy control over the Internet as an element of critical national infrastructure.

We can see this in attempts to control hate speech, cyber-bullying, spam, malware… and encryption. Under the headings of national security, counter-terrorism and the prevention of serious crime, numerous governments are proposing to limit the ability of malefactors to communicate securely and confidentially.

Some legislative moves seek to impose duties on companies to ensure that encrypted data can always be made accessible to law enforcement officers on presentation of a duly-served warrant. The organisation, increasingly, needs to be aware of the possibility of such a request, and consider its ability to respond.

The organisation's policy on that question may well need to cater for differences between the legal requirements in different jurisdictions.

2. Non-technical risk mitigations

Finally, a brief word to put cryptographic technology into perspective. It can be tempting to assume that technology, in general, is the solution to all business problems – and that cryptography, in particular, is the solution to all security risks. However, as IT security vendors have found for years, businesses will often find other, non-technical ways to mitigate risk.

For example, if the business risk is the possibility of a data breach exposing customer data, then one way to manage that risk is to insure against the cost of dealing with such a breach, rather than, for instance, incurring the cost and effort of encrypting the data as a pre-emptive protection.

Similarly, rather than investing in the cost and effort of ensuring that encrypted data can always be retrieved (even if some of the necessary keys are lost or damaged) some organisations may simply opt to lose the data and rely on procedural measures to cope with its loss.

The non-technical approach is not necessarily better or worse than applying technology: the two complement each other, and the balance between them is a business decision. Preferably, that business decision will be made on the basis of a clear understanding of the relative merits of the technical alternatives, and the goal of this paper is to help clarify that choice.

Questions to ask about non-technical factors

- Are we in a position to respond to law enforcement requests for access to secured data?
- What obstacles might there be to such a response?
- Are there any circumstances under which we would either deny such a request, or feel that we were legitimately unable to accede to it?
- Is access to corporate data appropriately protected when information assets or our employees cross jurisdictional boundaries?
- If we opt for non-technical mitigations of IT security risks, is that decision explicit and conscious?
- Are our users and partners aware of the need to secure the organisation's information assets, and of their role in doing so?
- What steps can we take to increase their awareness?
- Are users and partners educated in how to use the information security tools at their disposal, how to react to errors, and where to go for help?
- What steps can we take to ensure/improve their education?
- Overall, does cryptographic technology play a balanced and proportionate part in our organisation's security strategy?

Annex A: Very Short Glossary

This glossary is intentionally minimal. Its aim is to give brief definitions of the half dozen key concepts on which this paper is based.

Cryptography:	A group of related services (encryption, hashing, integrity checks) which, in combination, allow information to be secured against unauthorized use, access, or modification. In the field of information security, cryptography is applied in support of the functions and services defined below.
Encryption:	A reversible process for turning information into a form that conceals its meaning, thus maintaining its secrecy or confidentiality. The most common type of encryption is a cipher: a technique that uses secret keys as input to the reversible process, and which results in cipher-text which is practically indistinguishable from random data. Other types of encryption include codes (e.g. replacing one word with another) and steganography (hiding a message in other information).
Confidentiality:	The ability to store or exchange information in a form that renders it incomprehensible to a third party.
Integrity:	The ability to store or exchange information in such a way that a third party cannot modify it without detection.
Availability:	The ability to access information when it is needed, despite the possibility of operational disruptions, denial-of-service attacks, etc.
Authentication:	The ability to confirm an attribute asserted about an entity. For the purposes of this paper, authentication is the ability to confirm that an entity is who he/she/it claims to be (a valid user, a badge-holder, a corporate website, a specific named individual). Authentication is a precursor to authorization and access control: "now that I know who you are, I can look up what you are allowed to access on this system".

Annex B: Brief background on Public Key Infrastructure (PKI)

As noted above, data confidentiality services and data integrity services are both likely to introduce a requirement for use of a PKI.

For example: if your employees need to encrypt or sign emails, they will need PKI; if your website requires https, it relies on PKI; if you process card payments via your website, you will probably need PKI for compliance with PCI DSS (Payment Card Industry Data Security Standard). You may also have PKI-related requirements that arise out of your participation in government identity schemes, such as PIV (Personal Identity Verification) in the US, or eIDAS (Electronic Identification and Signature) in the European Union.

This annex looks briefly at some more detailed factors relating to PKI use. These aren't "questions for your CTO", as such, but should be taken into account in the overall risk analysis and deployment strategy for PKI-dependent functions in your organisation.

A primary function of the public keys in a PKI is to identify the entity you are communicating with (for instance, to guarantee that the https session in your browser really is with the website you intended to visit). In order to guarantee the ownership of a given public key, the key has to be "certified" by a trusted third party, or certificate authority (CA). These CAs form the basis of the public key infrastructure (PKI).

The most visible large-scale application of PKI technology is in support of encrypted browser sessions (https). To keep the PKI scalable, there need to be numerous CAs, and to ensure it secures the world-wide web, web browsers (and mobile devices) must incorporate lists of known and trusted CAs.

The PKI also depends on browsers/devices being able to tell if a public key or its certificate is no longer valid, so the infrastructure must also support certificate revocation lists (CRLs) and an online certificate status protocol (OCSP).

The resulting PKI, taken as a whole, has some serious drawbacks:

- Some CAs have proved unreliable, undermining, at a stroke, the certificates they issued and any sub-CAs they endorsed;
- Removing "bad" CAs from the lists held by browsers and devices takes time and cannot safely be left to users – so the system must be designed to allow this to be done remotely. Otherwise, devices and websites may continue to rely on certificates they should no longer trust.
- Users generally react unreliably to warnings about invalid certificates or CAs, so although the underlying mechanism may be working correctly, if it depends on users taking appropriate remedial action, it is likely to fail.
- PKI has achieved the greatest deployment volumes where it is kept away from the user: set-top boxes, cable modems, smart meters, and some mobile handset applications. However, insulating the technology from the user also means that any management of the PKI must be done remotely if it is to scale sufficiently.
- Some enterprises invest in mobile device management (MDM) solutions or remote device management (e.g. for PCs) to help mitigate this risk. However, if your enterprise depends on

embedded PKI in remote devices (such as industrial control systems, telecommunications infrastructure, smart meters, etc.), other management disciplines will be required.

Aside from helping secure browser sessions, PKI is used in support of a number of other security-related functions: signing documents to protect their integrity and authenticity; newer cryptographic applications such as signing the data that comprises a block chain; helping maintain the integrity of the Internet routing system (for example, DNSSEC); authenticating users to web applications and services; providing secure communication for applications (SSH). The kinds of imbedded, connected device that comprise the Internet of Things (IoT) are also very likely to incorporate PKI if they incorporate encryption technology.

The most common commercial products in support of PKI are Certificate Servers – the software that signs each public key and embeds it in a certificate, so that the key can safely be used for the purposes described above. However, the functionality of such products tends to focus on the generation of certificates and their later revocation. There is relatively little commercial software support for the management of keys and certificates in the intervening lifecycle.

There is also relatively little software support for managing the artefacts of a PKI (for instance, signed documents or archives).

PKI is relatively poorly integrated with mainstream email applications, and even if a user installs and configures the necessary components, doing something like sending a cryptographically signed email via a mailing list often "breaks" the signature, making it appear that the email has been maliciously altered even if it has not.

Applications sometimes also make "embedded" use of PKI, in the form of SSH (secure shell) – a protocol for securing network connections at the application or operating system level. This can result in unmanaged keys, for instance if a developer decides to code an SSH session into an application. In some instances, developers have done this and then failed to cater for the expiry of the keys used – so when the key expired, the application was suddenly and inexplicably unable to connect to the necessary server. The consequences can be severe: in one case, the application was unable to read a table of daily currency exchange rates, and the resulting error prevented a foreign exchange floor from trading until the problem was found and fixed.

In summary: public key encryption solves some practical problems of encryption deployment, but introduces others, including the need for a large infrastructure of trusted third parties. The technical tools of PKI do what they are supposed to, but the operational and auxiliary services around them are frequently immature or absent. Insulating the user from the technology helps speed deployment at scale but introduces challenges of remote management.