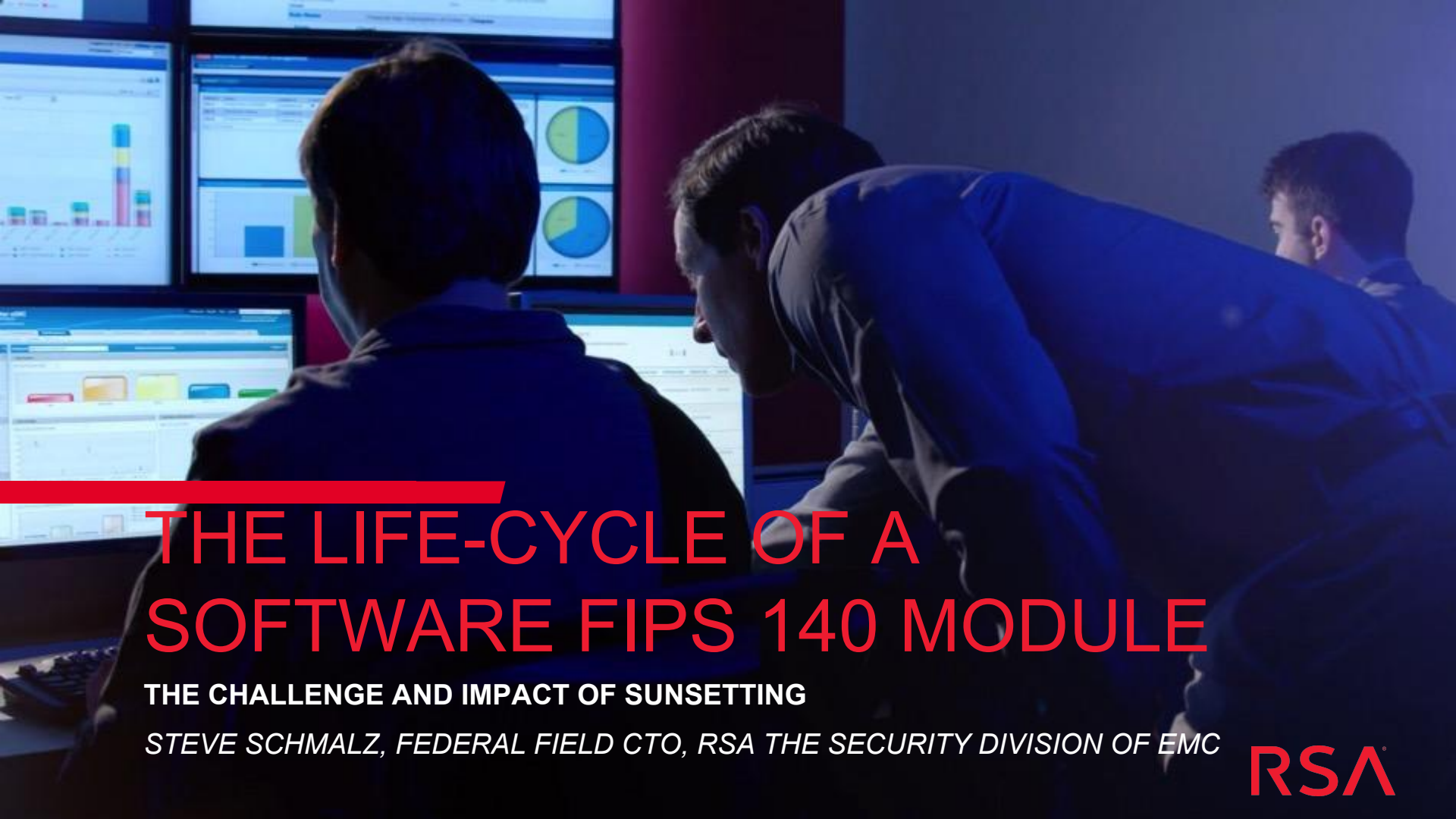
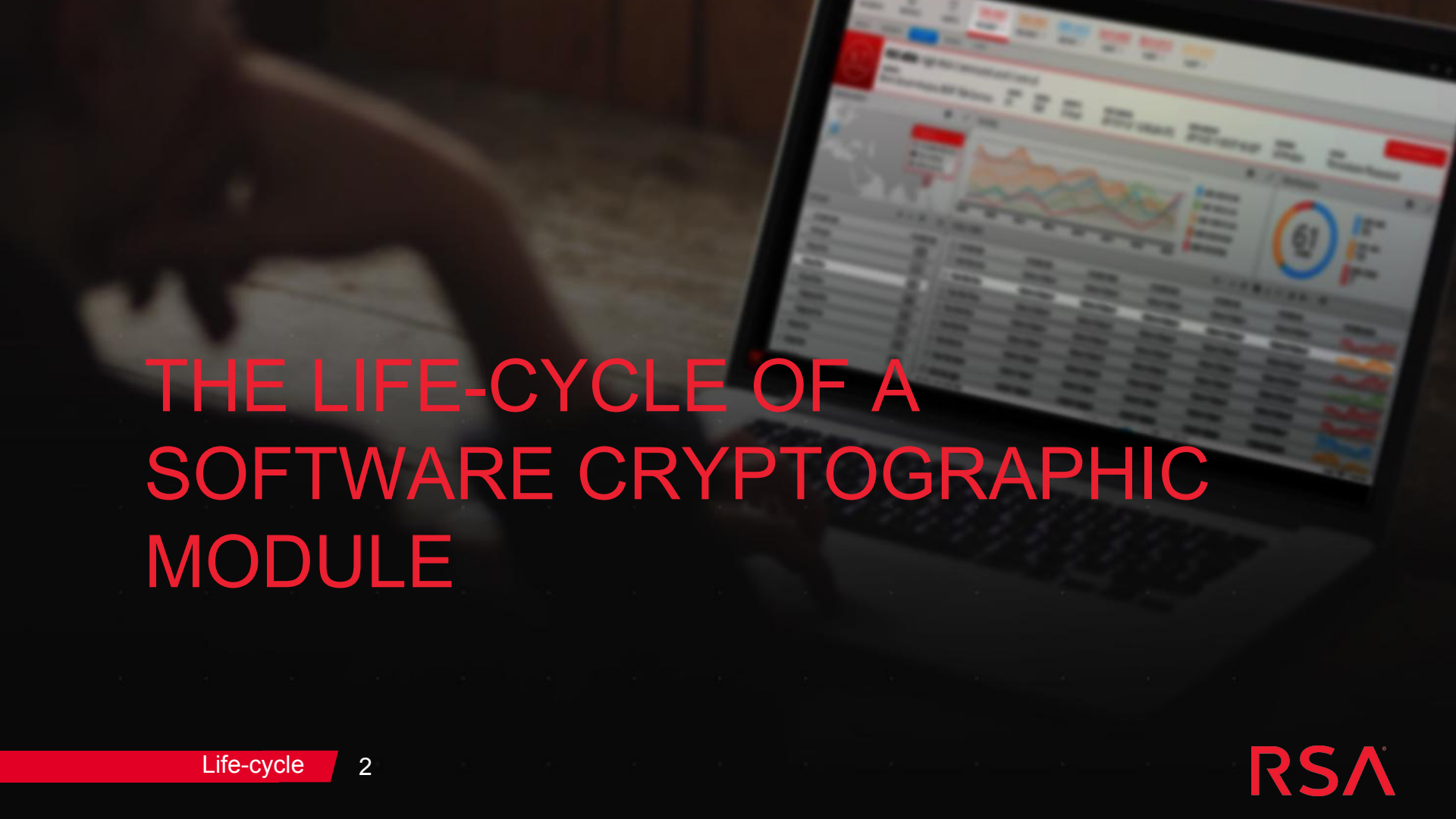


THE LIFE-CYCLE OF A SOFTWARE FIPS 140 MODULE

THE CHALLENGE AND IMPACT OF SUNSETTING

STEVE SCHMALZ, FEDERAL FIELD CTO, RSA THE SECURITY DIVISION OF EMC

RSA



THE LIFE-CYCLE OF A SOFTWARE CRYPTOGRAPHIC MODULE

RSA

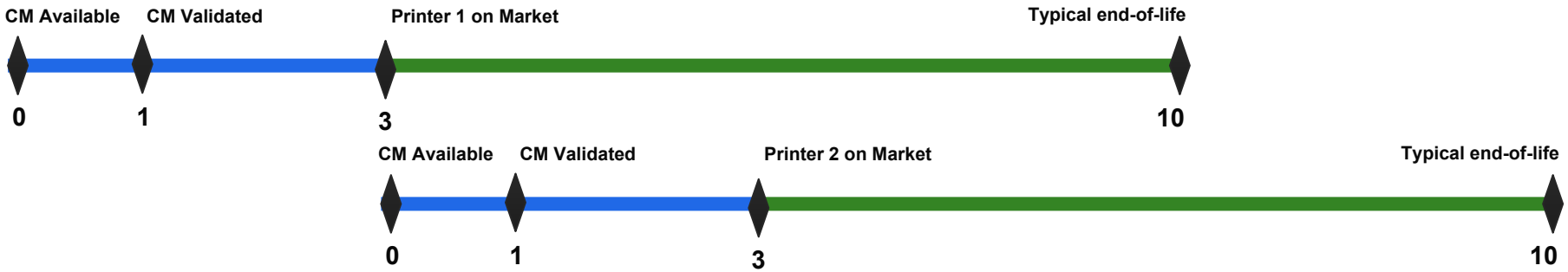
Life-cycle

- **Cryptographic modules are often OEMed**
  - From the date of validation OEMs may take 6-18 months to integrate the module into their product.
  - The new product may also be OEMed to another vendor…
- **Even after procurement by the ultimate end-user actual deployment could take months.**
- **And after deployment the end-user needs to use the module correctly and monitor its use to insure compliance.**
- **Points of Enforcement of FIPS 140 requirements**
  - The organization validating the module in order to meet customer requirement,
  - The ultimate end-user's procurement requirements,
  - Note – beyond Common Criteria very few mechanisms motivating/insuring the correct use of the FIPS 140 module after procurement.

RSA

Real World Use-case – Printer Companies

- Large corporate printers can be in use for up to 7 years.
- Development time usually runs 3 years.
- Thus time from the start of development to the end of life is around 10 years.
- Development of a new printer overlaps lifespan of older models.
- Integration of software modules require that the software interface be known at the beginning of development
- But development can run parallel to the last 6-months to year of module validation (that is after the lab is finished).
- Development and replacement (integration, QA etc.) of software modules takes 6 months to a year.



THE PROPOSED NEW SUNSETTING REQUIREMENT

RSA

Validation Sunsetting Policy

- Effective January 1st 2017.
  - By January 31st 2017, all validations with dates prior to January 1st 2012 will be moved from the Active Validation list to the Legacy Validation list.
  - Federal agencies can not procure from the legacy list.
  - Federal agencies must make a risk management decision on the continued use of the legacy module.
- Vendors may reinstate modules by
  - Reaffirming the validation of modules fully compliant to the standard and IG.
  - Or follow the most recent IG for the revalidation of Modules that require some maintenance changes.
- Vendors having issues (hardship cases) with the January 1, 2017 deadline should contact the CMVP who will work with them to minimize the impact.

RSA

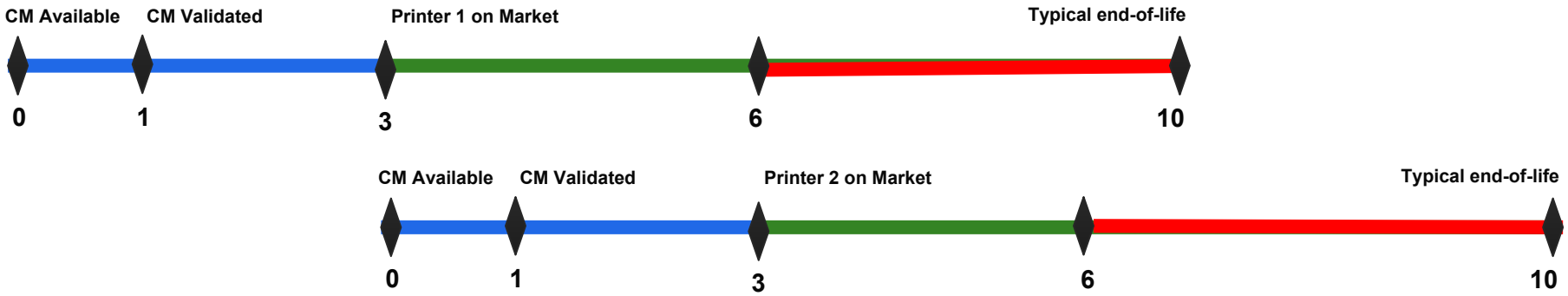
Impact of Sunsetting Requirement

- This may make software cryptographic modules out-of-date before some are ever deployed to end-users.
- End-user will only be motivated to look for an up to date certificate during procurement.
- Most organizations will not have the resources or motivation to monitor the status of the cryptographic models they use.
- The impact will fall mostly on the vendors building and OEMing the cryptographic modules with few requirements addressing the use of outdated modules by end-users.

RSA

Best Case Timeline for Sunsetting Impact on Printer Companies

- Printer hits the market and three years later the CM needs to be updated.
- It takes 6 months to a year to do integration and QA.
- This leaves a non-compliant printer in the field for 6 months to a year.
- Unless the printer company starts the replacement process 1 year earlier shortening the relevant life of the CM by a year.
- This is best case and if a new CM does not match the development timeline perfectly the delay is greater.
- Some end-users may elect to do nothing leaving a non-compliance printer in the field for 4-5 years.



THE REAL PROBLEM/SOLUTION

RSA

The Real Problem and Solution

- **"Significant" security issues in active CMs do need to be addressed**
  - Sometimes actual software vulnerabilities are found that require modifications forcing re-validation.
  - Other times access or use of some out-of-date algorithm or security parameter (i.e. key length) needs to be addressed or significant changes are made to the IG.
- **Why put an arbitrary 5-year sunsetting rule into place, when**
  - You can address a lot of security issues with configuration changes.
  - And the 5-year sunsetting rule doesn't actually address the real issue since it doesn't enforce any action by the end-user.
- **Work needs to be done to determine a more creative solution that better fits the modern cybersecurity landscape.**

RSA

Thank You – Questions?

Steve Schmalz
Federal Field CTO, RSA the Security Division of EMC
steve.schmalz@rsa.com

RSA