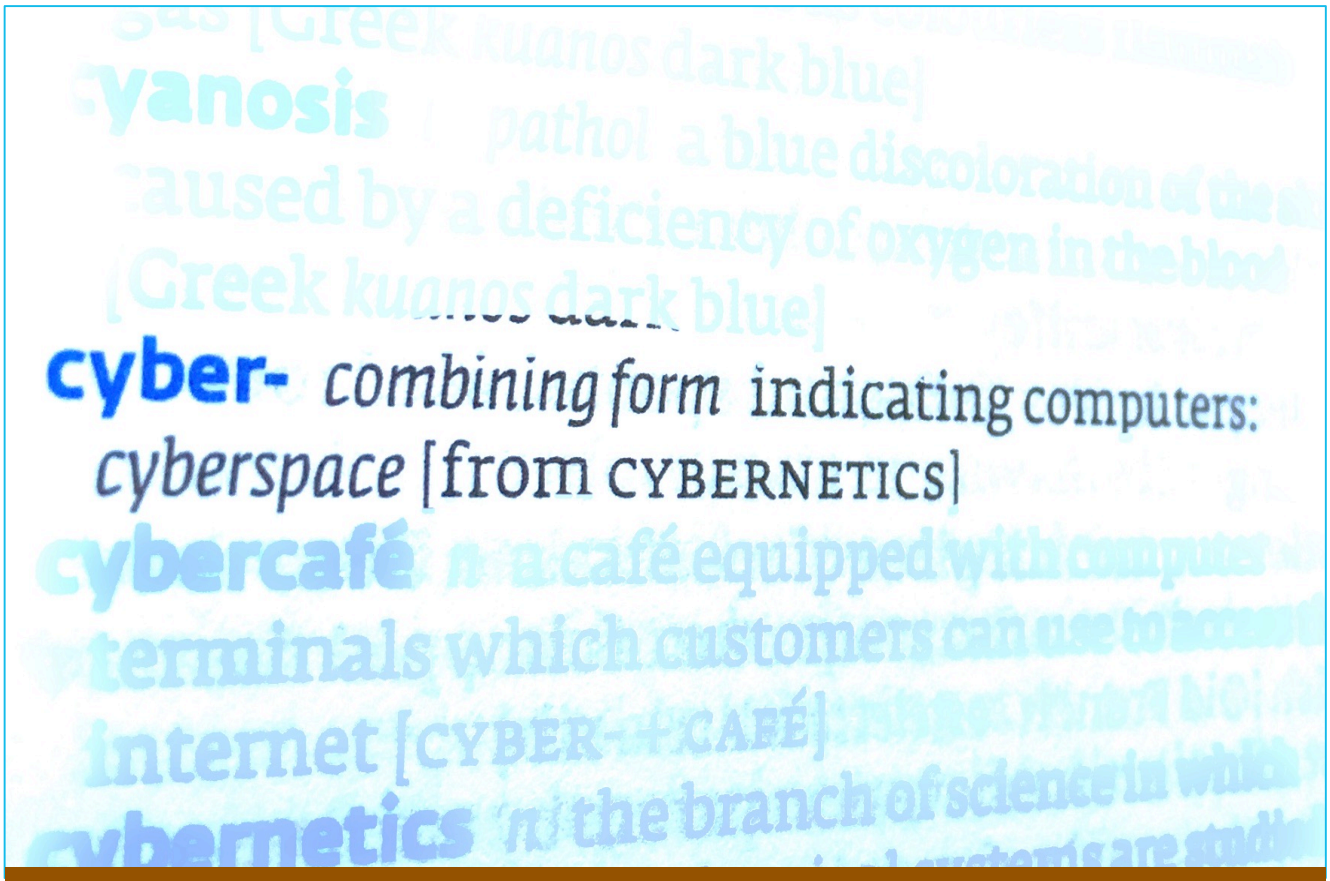

Cyber security basics for law firms

Guidance for law firms on governance, risk, and compliance basics to provide assurance on cyber security for in-house operations and to address clients' security concerns.

BrownGlock, 4th Floor, 86-90 Paul Street
London, EC2A 4NE | www.brownglock.com

Background

Cyber security is undoubtedly a hot topic for law firms and their clients. Security professionals now talk of a world where everyone should "*assume breach*"; assume that an attacker has breached your defences and is active within your firm.

Trust is the major currency that law firms use to gain and keep clients. Demonstrating trustworthiness in a world of "assume breach" is complex but can be achieved by getting the appropriate governance, risk, and compliance in place. (Successfully Adopting an 'Assume Breach' Mindset - Damballa, 2015)

Start with understanding the risks

At the very basic level, Information Security is about ensuring confidentiality, integrity, and availability (CIA) of information. In addition it is good management practice to provide accountability and assurance. (NIST, 2001)

A good place to start is to ask two questions:

1. What do you want to protect?
2. Why does it need protection?

Answering "what?" demands the identification and classification of information assets. Answering "why?" establishes the risks and

enables business justification for necessary controls to mitigate those risks.

Specifically for law firms the areas to focus on:

- Confidentiality of client information
- Protection of intellectual property
- Accuracy and integrity of matter management & billing
- Information interchange with clients

Get the basic controls right

Over the past 20 years Information Security has become a mature profession. Professional bodies such as (ISC)² offer training and enabling the sharing of best practice and a lively security professional community. (ISC2, 2015)

The SANS Institute was established in 1989 as a cooperative research and education organization. SANS maintains a top list of technical controls to establish and manage [http://www.sans.org/critical-security-controls]. These are considered best practice amongst security professionals. At the time of publication they were:

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
4. Continuous Vulnerability Assessment and Remediation
5. Malware Defences
6. Application Software Security
7. Wireless Access Control
8. Data Recovery Capability
9. Security Skills Assessment and Appropriate Training to Fill Gaps
10. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
11. Limitation and Control of Network Ports, Protocols, and Services
12. Controlled Use of Administrative Privileges
13. Boundary Defence
14. Maintenance, Monitoring, and Analysis of Audit Logs
15. Controlled Access Based on the Need to Know
16. Account Monitoring and Control
17. Data Protection
18. Incident Response and Management
19. Secure Network Engineering
20. Penetration Tests and Red Team Exercises

(SANS, 2015; ISC2, 2015)

Issues such as BYoX [Bring your own device/app/cloud/network…], the move to hybrid Cloud computing and the need to share sensitive information with clients and affiliates in multiple geographies complicate the implementation of these security controls.

However, implementation and adherence to the controls has been shown to be effective against the majority of attempted breaches. As SANS say:

"The Critical Security Controls focuses first on prioritizing security functions that are effective against the latest Advanced Targeted Threats, with a strong emphasis on "What Works" - security controls where products, processes, architectures and services are in use that have demonstrated real world effectiveness."

Enhanced basics for law firms

None of the controls above are specific to law firms nor do they directly address the headline issue of advanced persistent threats (APTs) which allow determined attackers to infiltrate, explore, and in some cases control information assets for considerable periods of time before detection (if they are detected at all). (Gartner, 2014)

According to the M-trends report from FireEye, despite one organisation being breached for over eight years, the time it takes organisations to detect that they have been compromised dropped to 205 days in 2014, down from 229 days in 2013 and 243 days in 2012. (Mandiant, 2015)

Yet the report said that it is becoming harder for organisations to detect that they have been breached, with only 31 per cent of organisations discovering that they were breached via their own resources; down from 33 per cent in 2013 and 37 per cent in 2012.

Trust is such a hygiene issue for law firms that enhanced protection against information disclosure should be a priority. Services to consider:

a) Cyber threat intelligence

Law firms cast a digital shadow: unintentionally exposed personal, technical or organizational information that is often highly confidential, sensitive or proprietary. As well as damaging the brand, a digital shadow can leave the firm vulnerable to espionage and competitive intelligence. Worse still, criminals and hostile groups can exploit a digital shadow to find the firm's weak points and launch a targeted cyber attack.

Cyber threat intelligence providers look for information leaking out about your business. They use search and analysis algorithms to track information you might not know is public. (Wired, 2015)

b) Deception, decoys and breach detection

Gartner has called 2015 "the year of offensive deceptions". Deception technology from organisations such as Cymmetria Inc. fulfils two main requirements: diverting attackers away from information assets to decoys where they can be persuaded to expose their attack methods; identifying breaches with high confidence in contrast to the large number of alarms from currently deployed Security Information and Event Management platforms (SIEM). In addition, it is possible to generate signatures from the attack methods used, even though they are using previously unknown methods, so that other control points can detect and stop further attacks. (Cymmetria Inc., 2015)

Establishing effective governance

The IT profession has built a number of effective frameworks for managing IT. In the context of Cyber GRC we recommend concentration on the following:

ISACA (previously the Information Systems Audit and Control Association) was incorporated in 1969 by a small group of individuals who recognized a need for a centralized source of information and guidance in the growing field of auditing controls for computer systems. Today, ISACA serves 140,000 professionals in 180 countries. The **COBIT** (Control Objectives for IT) framework from ISACA is the leading framework for governance and management of IT. (ISACA, 2015)

ITIL (IT Information Library) is the most widely accepted approach to IT service management in the world. ITIL advocates that IT services are aligned to the needs of the business and support its core processes. It provides guidance to organizations and individuals on how to use IT as a tool to facilitate business change, transformation and growth.

The ITIL best practices are currently detailed within five core publications:

- ITIL Service Strategy
- ITIL Service Design
- ITIL Service Transition
- ITIL Service Operation
- ITIL Continual Service Improvement.

These five volumes map the entire ITIL Service Lifecycle, beginning with the identification of customer needs and drivers of IT requirements, through to the design and implementation of the service and finally, the monitoring and improvement phase of the service. (Axelos, 2015)

Where COBIT is about establishing controls, ITIL addresses the development and delivery of services to the business.

For IT security, there has been much work done in enshrining best practice for governance in cyber security into **ISO/IEC 27001 2013**. (International Organization for Standardization, 2015)

The choice of governance framework(s) will be driven largely by compliance requirements. Few law firms have achieved accreditation to a formal standard but there is considerable interest amongst firms, especially those operating in the financial markets of New York and London. (Intapp, 2015)

Compliance: Yours, your suppliers' and your clients'

Governance and compliance are inextricably interlinked, as compliance usually requires some form of accreditation to a standard. Many clients, especially those in regulated industries such as healthcare, financial services, and government, are looking to all of their supply chain to be auditable against an agreed standard such as ISO 27001. Law firms should respond in two ways:

a) Be 'audit-ready' by adopting controls in line with the standards that your customers have adopted.

Whether or not your firm decides to seek formal ISO accreditation, the preparation exercise to define and document controls will enable your firm to accommodate audit request from your customers.

b) Impose compliance on your supply chain

Law firms can ease the burden of compliance by sourcing services from vendors that have gained accreditation and/or are members of a recognized security group e.g. the Cloud Security Alliance for Cloud vendors.

Seek out like-minded law firms and industry groupings

Industry bodies such as the Law Society and the American Bar Association provide forums to discuss cyber security issues and share best practice.

Cyber GRC as a competitive advantage

There is a logical step between investing in 'basic' security as a cost of doing business and making an additional investment to become accredited and a recognized leader in Cyber GRC. As a leader, not only will you be able to differentiate in regulated industries but you can also use your in-house experience to support your GRC practice in their client engagements.

Summary & Recommendations

Getting the basics right is a question of knowing what you want to protect, and why. Providing effective Cyber GRC for a law firm both mitigates business risks and allows the firm to differentiate.

We recommend a three-step approach to Cyber GRC:

1. Establish a baseline of the firms current Cyber GRC posture and effectiveness of the controls in place
2. Match the governance framework to the compliance requirements on the firm, taking advantage of managed services
3. Implement any required new controls and seek appropriate accreditation.

Bibliography

Axelos. (2015). *ITIL® - IT Service Management*. Retrieved from AXELOS Global Best Practice: https://www.axelos.com/best-practice-solutions/itil

BrownGlock. (2015). *Intelligence and Expertise for Lawyers*. Retrieved from BrownGlock: https://brownglock.com

Cymmetria Inc. (2015). *Maze Runner.* Retrieved from Cymmetria: http://www.cymmetria.com/maze-runner/

Gartner. (2014). *Best Practices for Mitigating Advanced Persistent Threats.* Retrieved from MIIS Cyber Initiative: http://sites.miis.edu/cysec/files/2014/01/Best-Practices-for-Mitigating-Advanced-Persistent-Threats.pdf

Intapp. (2015). *ISO Readiness*. Retrieved from Intapp: http://www.intapp.com/services/risk/iso-readiness

International Organization for Standardization. (2015). *ISO 27001 - Information security management*. Retrieved from ISO - International Organization for Standardization: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

ISACA. (2015). *COBIT Framework.* Retrieved from Enterprise IT Management - ISACA: https://cobitonline.isaca.org

ISC2. (2015). *(ISC)² - IT Certification and Security Experts*. Retrieved from (ISC)² - IT Certification and Security Experts: https://www.isc2.org

Mandiant. (2015, March). *M-Trends Report.* Retrieved from https://www2.fireeye.com/WEB-2015-MNDT-RPT-M-Trends-2015_LP.html

NIST. (2001, December). *Underlying Technical Models for Information Technology Security*. Retrieved from National Institute of Standards and Technology: http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf

SANS. (2015). *Critical Security Controls - Version 5*. Retrieved from SANS: http://www.sans.org/critical-security-controls

Successfully Adopting an 'Assume Breach' Mindset - Damballa. (2015). Retrieved from Advanced Persistent Threat Detection and Advanced Malware Detection: https://www.damballa.com/in-the-spotlight-successfully-adopting-the-assume-breach-posture/

Wired. (2015, January). *Digital Shadows wants to keep you safe on the net.* Retrieved from Wired: http://www.wired.co.uk/magazine/archive/2015/04/start/digital-shadows

About the Author

With over 30 years in IT and telecoms, Peter Glock specialises in building new, and transforming existing businesses. Wide ranging experience of establishing, developing and promoting IT and Telecoms related businesses for large enterprise and multinational markets, particularly in professional services and finance segments. In 1999 he co-founded the managed security services business for Equant (later Orange Business Services) and is a regular speaker on IT subjects, particularly about governance, risk and compliance issues associated with business transformation.

Contact: peter.glock@brownglock.com

About BrownGlock

Brown Glock Creissen Rothwell-Brooks Ltd (BrownGlock, 2015) was founded by a group of experienced IT professionals to address the challenges of transformation for the legal sector. The legal sector is predicted to experience unprecedented change and pressure to consolidate as business activities undergo digital transformation. Using the experience of the BrownGlock team we aim to bring intelligence and expertise to law firms and the wider legal sector.