1.1.	Cyberkriminalität: Alle Formen der Datenkriminalität. Der größte Schaden für Unternehmen entsteht beim Diebstahl sensibler Daten und der Sabotage von IT-Systemen. Sabotage von IT-Systemen führt dazu, dass sich Prozesse nicht mehr steuern lassen: Produktion, Einkauf, Verkauf, Lagerhaltung, Buchführung. Das führt zu Umsatzeinbußen und Verlusten. – Datenklau kann Betriebsgeheimnisse und sensible Bereiche betreffen, z. B. Forschung und Entwicklung, Produktionsverfahren, Grundlagen der Kalkulation, aber auch Daten von Kunden und Lieferanten einschließlich der Passwörter. Spionage durch Konkurrenten bleibt oft längere Zeit unentdeckt. Die Gefahr für Unternehmen ist groß. Eindeutig betroffen ist etwa die Hälfte der Unternehmen, ein weiteres Viertel hat Anhaltspunkte dafür. Besonders lohnende Ziele sind technologisch führende Branchen (Automobile, Chemie / Pharma), Branchen mit vielen Kundendaten (Handel, Medien, Gesundheit) und Finanz- und Versicherungswesen wegen des Zugriffs auf Konten. (S. 92 f.)	5 P.
1.2.	• Industrie 4.0: Digitale Vernetzung und Kommunikation zwischen Menschen (Bedienungspersonal, Lieferanten, Kunden), Maschinen und Produkten, d. h. Verzahnung von Produktions- und Informationstechnik. Wird als vierte industrielle Revolution gesehen (Name!). (S. 54) • Industrie 4.0 erzeugt große Datenmengen, die zwischen den Beteiligten über das Internet ausgetauscht werden. Diese Daten sind sensibel, weil auf ihnen die Steuerung der Produktion beruht. Wer sich unbefugt Zugang zu diesen Daten verschaffen kann, kann Produktionsprozesse lahmlegen oder manipulieren. Darum sind sehr hohe Sicherheitsstandards und Verschlüsselungstechniken nötig, die von allen (!) Beteiligten eingehalten werden müssen. (S. 95 ff.)	5 P.
2.1.	• Malware: Manipulation oder Löschen von Dateien, heimliches Installieren von Spyware, Kapern von Rechnern. • Phishing: Ausspionieren von Zugangsdaten über E-Mails oder gefälschte Webseiten. • Weitergabe privater Daten, besonders in sozialen Netzwerken: Werden vom Betreiber legal ausgewertet, verknüpft und zu Geschäftszwecken verwendet bzw. weiterverkauft. • Hacken der Server von Internet-Dienstleistern, um an Nutzerdaten und Passwörter zu kommen. • Betrug beim Online-Kauf. (S. 92 f., 96 f.)	3 P.
2.2.	• Professionellen Virenscanner und Firewall verwenden und laufend aktualisieren, damit keine Schadsoftware (Viren, Trojaner) auf den Rechner geladen wird. • Sichere Passwörter verwenden und für jede Anwendung ein anderes Passwort nutzen, damit ein Datenleck bei einem Online-Dienst nicht den Zugang zu anderen privaten Accounts ermöglicht. • Nur zwingend erforderliche private Daten weitergeben. Ggf. auf die Nutzung von Apps verzichten, um die kommerzielle Verwendung der eigenen Daten zu begrenzen. • Allen E-Mails misstrauen. Beim geringsten Zweifel nicht öffnen. Grund: siehe Virenscanner. • Wichtige Daten verschlüsseln. (S. 96 f.) Zusätzlich: Beschreibung des eigenen Wegs (individuelle Lösungen).	6 P.
3.1.	Beispiele aus der Erfahrungswelt des Schülers, z. B. über • Vergabe von Arbeitspaketen an freie Mitarbeiter, Selbstständige oder andere Unternehmen außer Haus, die im Datenverbund mit dem Auftraggeber arbeiten. Kann sich auf traditionelle Tätigkeiten wie Buchhaltung, Kundendienst, Hotline beziehen, aber auch auf neue Tätigkeiten wie Webdesign oder Programmiertätigkeiten. • Datenaustausch und Telefonkonferenzen zwischen Mitarbeitern und Externen weltweit; Nutzung von Clouds. • Steuerung und Kontrolle von Prozessen (z. B. Maschinen) extern über Datenleitungen, z. B. Windkraftanlagen, Kraftwerke, Schleusen, Bahnstrecken … • Fernwartung von Geräten (Maschinen, Computer). (S. 56 ff.)	4 P.
3.2.	+ Bessere Vereinbarkeit von Beruf und Familie durch Arbeit zu Hause und freiere Zeiteinteilung. + Wegfall von Arbeitswegen (Zeitgewinn, Kostenersparnis). – Grenze zwischen Arbeit und Privatleben verschwindet: Überschneidung der Anforderungen in Familie und Beruf; Ausdehnung des Arbeitstags. – Im Home Office ist die Datensicherheit nicht gewährleistet (kein geschützter Raum). – Einbindung in den betrieblichen Kommunikationsprozess schwierig, wenn nur im Home Office gearbeitet wird. Abwägung: Ob Vor- oder Nachteile überwiegen, hängt von der persönlichen und familiären Situation des Arbeitnehmers ab und von den Bedingungen, die der Arbeitgeber festlegt: Zeiten der Erreichbarkeit, zeitliche Flexibilität, Ausstattung des Home Office. (S. 32, 59)	4 P.
3.3.	• Technologisch sind immer mehr Arbeiten im Home Office möglich (vgl. Industrie 4.0). • Veränderungen der Unternehmenskultur und der Führungsstile: Keine Anwesenheitskultur, sondern ein ergebnisorientiertes Arbeiten. • Rollenwandel in der Familie: Mehr Väter wollen Nähe zur Familie. • Ein Plus für Unternehmen bei der Gewinnung von Personal. (S. 32, 57, 59)	3 P.
Erreichbar		30 P.